HP StorageWorks

All-in-One Storage System

user guide

Part number: 440583-005
First edition: February 2008

Legal and notice information

© Copyright 2006, 2008 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, Windows, Windows XP, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group.

Contents

About this guide 15
Intended audience 15
Related documentation 15
Document conventions and symbols 15
Rack stability 16
HP technical support 17
Customer self repair 17
Product warranties 17
Subscription service 17
HP websites 18
Documentation feedback 18

1 Installing and configuring the server 19
Setup overview 19
Planning for installation 19
Planning a network configuration 20
Configuration checklist 20
Installing the server 21
Locating and writing down the serial number 21
Checking kit contents 21
Powering on the server 22
Factory image 22
Physical configuration 22
Default boot sequence 23
Accessing the All-in-One Management Console 23
Using the direct attach method 23
Using the remote browser method 24
Using the Remote Desktop method 26
Logging off and disconnecting 27
Telnet Server 27
Enabling Telnet Server 27
Using remote management methods 28
Using the Lights-Out 100 method 28
Using the Integrated Lights-Out 2 method 29
Configuring the server on the network 30
Before you begin 30
Running the Rapid Startup Wizard 32
Completing system configuration 32
Installing the All-in-One Storage Manager Agent 33
Installing the All-in-One Storage Manager Agent on network application servers 33

2 Storage system components 35
HP StorageWorks 400r All-in-One Storage System 35
HP StorageWorks 400t All-in-One Storage System 37

HP StorageWorks 600 All-in-One Storage System 40
SAS and SATA hard drive LEDs 43

3 Storage management overview 45
Storage management elements 45
Storage process management example 45
Physical storage elements 46
Arrays 47
Fault tolerance 48
Online Spares 48
Logical storage elements 48
Logical drives (LUNs) 48
Partitions 49
Volumes 49
File system elements 50
File sharing elements 50
Volume Shadow Copy Service overview 50
Using storage elements 51
Network adapter teaming 51
Management tools 51
HP Systems Insight Manager 51
Management Agents 51
All-in-One Storage Manager 52
Software requirements 52
Software support 52
Storage management infrastructure 53
Managing storage for application servers 53
Managing storage for shared folders 54
About the user interface 56
Menu bar 56
Toolbar 56
Navigation pane 56
Content pane 56
Actions pane 57
Defining user interface options 58
Add an All-in-One Storage System 59
Remove an All-in-One Storage System 59

4 Hosting storage for applications and shared folders 61
Using the Host an Exchange Storage Group Wizard 62
Entering a name of a server that hosts Exchange 62
Selecting Exchange storage group components 63
Local Continuous Replication (LCR) 63
Using the Create a Shared Folder Wizard 64
Naming a shared folder 64
Setting permissions for a shared folder 64
Using the Host a SQL Server Database Wizard 65
Selecting a server that hosts SQL Server 65
Selecting SQL Server database components 65
Selecting a database workload type 66
Using the Host a User-Defined Application Wizard 67
Choose type of application 68
Entering an application name 68
Using the Create a Virtual Library Wizard 68

Accessing the Virtual Library Wizard 68
Configure your virtual library 68
Allocating space for components 69
Selecting advanced configuration settings 71
Selecting data protection 76
Reviewing task summary and scheduling tasks 78
Monitoring task completion status 79
Cancelling tasks 79
Migrating user-defined application data from a remote application 80

5 Data protection 81
Data Protection Window 81
Selecting local or alternate backup 81
Managing snapshots and backups 82
Snapshots 82
Scheduling snapshots 82
Taking snapshots 82
Exposing a snapshot 83
Unexposing a snapshot 83
Reverting data to snapshots 83
Scheduling and running backups 84
Managing backups 84
Restoring data from backups 84
Selecting the restore destination 85
Launching DPX 85
Using DPX to restore data 85
Setting the password for the ASMbackup user account 85
Installing Data Protector Express on other devices 86

6 Managing storage 89
Increasing or reducing the allocated storage 89
Changing the percent full warning threshold 90
Removing application areas from view 91
Changing permissions, names, descriptions, or paths of shared folders 91
Deleting shared folders 92

7 Monitoring storage 93
Application View 93
Accessing application and shared folder properties 94
Data Protection 103
Storage View 105
Accessing storage area properties 106
Application Server View 108
Accessing application server properties 108
Storage Utilization View 110

8 Troubleshooting, servicing, and maintenance 111
Troubleshooting the storage system 111
Operating system problems and resolutions 111
Application software problems 112
SQL Server errors 112
ASM alerts 112
Recovering from logical disk failure 117

Maintenance updates 117
System updates 117
Troubleshooting resources 117
HP web site 117
Storage system documentation 118
Subscriber's Choice 118
White papers 118
Firmware updates 118
WEBES (Web Based Enterprise Services) 118
Certificate of Authenticity 119

9 System recovery 121
The System Recovery DVD 121
To restore a factory image 121
Systems with a DON'T ERASE partition 121
Managing disks after a restoration 121

A File server management 123
New or improved file services features in Windows Storage Server 2003 R2 123
Storage Manager for SANs 123
Single Instance Storage 123
Search enhancements 124
File Server Resource Manager 124
Windows SharePoint Services 124
HP All-in-One Management Console 124
File services management 125
Configurable and pre-configured storage 125
Storage management utilities 126
Array management utilities 126
Array Configuration Utility 126
Disk Management utility 127
Guidelines for managing disks and volumes 127
When managing disks and volumes: 127
Scheduling defragmentation 128
Disk quotas 128
Adding storage 129
Expanding storage 129
Extending storage using Windows Storage Utilities 130
Expanding storage using the Array Configuration Utility 130
Volume shadow copies 131
Shadow copy planning 131
Identifying the volume 131
Allocating disk space 132
Identifying the storage area 133
Determining creation frequency 133
Shadow copies and drive defragmentation 133
Mounted drives 134
Managing shadow copies 134
The shadow copy cache file 134
Enabling and creating shadow copies 136
Viewing a list of shadow copies 136
Set schedules 136
Viewing shadow copy properties 137
Redirecting shadow copies to an alternate volume 137

Disabling shadow copies 138
Managing shadow copies from the storage system desktop 138
Shadow Copies for Shared Folders 139
SMB shadow copies 140
NFS shadow copies 141
Recovery of files or folders 141
Recovering a deleted file or folder 141
Recovering an overwritten or corrupted file 142
Recovering a folder 142
Backup and shadow copies 143
Shadow Copy Transport 143
Folder and share management 144
Folder management 144
Share management 150
Share considerations 150
Defining Access Control Lists 151
Integrating local file system security into Windows domain environments 151
Comparing administrative (hidden) and standard shares 151
Managing shares 152
File Server Resource Manager 152
Quota management 152
File screening management 152
Storage reports 153
Other Windows disk and data management tools 153
Additional information and references for file services 153
Backup 153
HP StorageWorks Library and Tape Tools 153
Antivirus 153
Security 154
More information 154

B Print services 155
Microsoft Print Management Console 155
New or improved HP print server features 155
HP Web Jetadmin 155
HP Install Network Printer Wizard 155
HP Download Manager for Jetdirect Print Devices 155
Microsoft Print Migrator Utility 155
Network printer drivers 156
Print services management 156
Microsoft Print Management Console 156
HP Web Jetadmin installation 156
Web-based printer management and Internet printing 156
Planning considerations for print services 157
Print queue creation 157
Sustaining print administration tasks 158
Driver updates 158
Print drivers 158
User-mode vs. kernel-mode drivers 158
Kernel-mode driver installation blocked by default 158
HP Jetdirect firmware 158
Printer server scalability and sizing 159
Backup 159
Best practices 159

Troubleshooting 160
Additional references for print services 160

C Microsoft Services for Network File System (MSNFS) 161
MSNFS Features 161
UNIX Identity Management 161
MSNFS use scenarios 162
MSNFS components 162
Administering MSNFS 163
Server for NFS 163
User Name Mapping 168
Microsoft Services for NFS troubleshooting 169
Microsoft Services for NFS command-line tools 169
Optimizing Server for NFS performance 170
Print services for UNIX 170

D Other network file and print services 173
File and Print Services for NetWare (FPNW) 173
Installing Services for NetWare 173
Managing File and Print Services for NetWare 174
Creating and managing NetWare users 175
Adding local NetWare users 176
Enabling local NetWare user accounts 176
Managing NCP volumes (shares) 177
Creating a new NCP share 178
Modifying NCP share properties 178
Print Services for NetWare 178
Point and Print from Novell to Windows Server 2003 178
Additional resources 179
AppleTalk and file services for Macintosh 179
Installing the AppleTalk protocol 179
Installing File Services for Macintosh 179
Completing setup of AppleTalk protocol and shares 179
Print services for Macintosh 180
Installing Print Services for Macintosh 180
Point and Print from Macintosh to Windows Server 2003 180

E Configuring storage system for Web access (optional) 181
Setting up an Internet connection 181

F Regulatory compliance and safety 183
Federal Communications Commission notice 183
Class A equipment 183
Class B equipment 183
Declaration of conformity for products marked with the FCC logo, United States only 184
Modifications 184
Cables 184
Laser compliance 184
International notices and statements 185
Canadian notice (Avis Canadien) 185
Class A equipment 185
Class B equipment 185
European Union notice 185

BSMI notice 186
Japanese notice 186
Korean notice A&B 186
Class A equipment 186
Class B equipment 186
Safety 187
Battery replacement notice 187
Taiwan battery recycling notice 187
Power cords 187
Japanese power cord notice 188
Electrostatic discharge 188
Preventing electrostatic discharge 188
Grounding methods 188
Waste Electrical and Electronic Equipment (WEEE) directive 188
Czechoslovakian notice 188
Danish notice 189
Dutch notice 189
English notice 189
Estonian notice 190
Finnish notice 190
French notice 190
German notice 190
Greek notice 191
Hungarian notice 191
Italian notice 191
Latvian notice 191
Lithuanian notice 192
Polish notice 192
Portuguese notice 192
Slovakian notice 193
Slovenian notice 193
Spanish notice 193
Swedish notice 193

Glossary 195

Index 199

Figures

1 Internet options screen 25
2 HP StorageWorks 400r All-in-One Storage System front panel 35
3 HP StorageWorks 400r All-in-One Storage system rear panel 36
4 AiO400t front panel (bezel on) 38
5 AiO400t front panel (bezel off) 39
6 AiO400t rear panel 39
7 HP StorageWorks 600 All-in-One Storage System front panel 41
8 HP StorageWorks 600 All-in-One Storage System rear panel 42
9 SAS/SATA hard drive LEDs 43
10 Storage process management example 46
11 Configuring arrays from physical drives 47
12 RAID 0 (data striping) (S1-S4) of data blocks (B1-B12) 47
13 Two arrays (A1, A2) and five logical drives (L1 through L5) spread over five physical drives 49
14 Application storage infrastructure 54
15 Shared folder storage infrastructure 55
16 ASM main window 56
17 Storage Allocation page 70
18 Example of alert 113
19 System administrator view of Shadow Copies for Shared Folders 134
20 Shadow copies stored on a source volume 135
21 Shadow copies stored on a separate volume 135
22 Accessing shadow copies from My Computer 139
23 Client GUI 140
24 Recovering a deleted file or folder 142
25 Properties dialog box, Security tab 145
26 Advanced Security settings dialog box, Permissions tab 146
27 User or group Permission Entry dialog box 147
28 Advanced Security Settings dialog box, Auditing tab 148
29 Select User or Group dialog box 148
30 Auditing Entry dialog box for folder name NTFS Test 149
31 Advanced Security Settings dialog box, Owner tab 150

32 File and Print Services for NetWare dialog box 175
33 New User dialog box 176
34 NetWare Services tab 177
35 Automatic configuration settings 181
36 Proxy server settings 182

Tables

1 Document conventions 15
2 Network access methods 19
3 Installation and Configuration checklist 20
4 AiO Configurations 22
5 Server configuration steps 30
6 HP StorageWorks 400r All-in-One Storage System front panel components 35
7 HP StorageWorks 400r All-in-One Storage System rear panel components 36
8 AiO400t front panel components (bezel on) 38
9 AiO400t front panel components (bezel off) 39
10 AiO400t rear panel components 39
11 HP StorageWorks 600 All-in-One front panel components 41
12 HP StorageWorks 600 All-in-One Storage System rear panel components 42
13 SAS and SATA hard drive LED combinations 43
14 Summary of RAID methods 48
15 Software support 52
16 Actions pane quick reference 57
17 Selecting storage group components to host 63
18 Selecting database components to host 66
19 Advanced window items 72
20 Descriptions of RAID levels 73
21 Operating status: Exchange properties 95
22 Details tab: Exchange storage group properties 95
23 Storage tab: Exchange storage group component properties 95
24 Mail Store tab: Exchange storage group component properties 96
25 Public Store tab: Exchange storage group component properties 97
26 Log tab: Exchange storage group component properties 97
27 Operating status: Shared folder properties 98
28 Storage tab: Shared folder properties 104
29 Operating status: SQL Server properties 100
30 Storage tab: SQL Server database component properties 100
31 Data File tab: SQL Server database component properties 101
32 Log tab: SQL Server database component properties 101

33 Operating status: User-defined application properties 102
34 Storage tab: User-defined application properties 102
35 Operating status: Data Protection properties 103
36 Storage tab: Shared folder properties 104
37 Storage tab: Shared folder properties 104
38 Virtual Library Properties 105
39 Operating status: General tab 106
40 Storage tab: HP All-in-One Storage System logical disk properties 107
41 Storage tab: HP All-in-One Storage System volume properties 107
42 Operating status: Application server volume properties 109
43 Storage tab: Application server volume properties 109
44 Operating system problems 111
45 Alert descriptions 113
46 Tasks and utilities needed for storage system configuration 125
47 Authentication table 164
48 MSNFS command-line administration tools 169

About this guide

This guide provides information for setting up, configuring, and administering the HP StorageWorks All-in-One Storage Systems.

- HP StorageWorks 400r All-in-One Storage System
- HP StorageWorks 400t All-in-One Storage System
- HP StorageWorks 600 All-in-One Storage System

This guide is available on the HP web site and is also provided as a PDF document on the HP StorageWorks All-in-One Storage System documentation CD.

Intended audience

This guide is intended for use by network and IT professioinals who are experienced with the following:

- Microsoft ®administrative procedures
- System and storage configurations

Related documentation

The following documents provide related information:

- *HP StorageWorks All-in-One Storage System Quick Start Instructions*
- *HP Integrated Lights-Out 2 User Guide*
- *HP StorageWorks All-in-One Storage System Release Notes*
- *HP StorageWorks Data Protector Express User's Guide and Technical Reference*

You can find these documents from the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

In the Storage section, click **Disk Storage Systems** and then select your product.

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Blue text: Table 1	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box

Convention	Element
	• GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

WARNING!

Indicates that failure to follow directions could result in bodily harm or death.

CAUTION:

Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT:

Provides clarifying information or specific instructions.

NOTE:

Provides additional information.

TIP:

Provides helpful hints and shortcuts.

Rack stability

Rack stability protects personnel and equipment.

⚠ WARNING!

To reduce the risk of personal injury or damage to equipment:

- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install stabilizing feet on the rack.
- In multiple-rack installations, fasten racks together securely.
- Extend only one rack component at a time. Racks can become unstable if more than one component is extended.

HP technical support

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Customer self repair

HP customer self repair (CSR) programs allow you to repair your StorageWorks product. If a CSR part needs replacing, HP ships the part directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your HP-authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider. For North America, see the CSR website:

http://www.hp.com/go/selfrepair

Product warranties

For information about HP StorageWorks product warranties, see the warranty information website:

http://www.hp.com/go/storagewarranty

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/e-updates

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

HP websites

For additional information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.hp.com/service_locator
- http://www.hp.com/support/manuals
- http://www.hp.com/support/downloads

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to storagedocsFeedback@hp.com. All submissions become the property of HP.

1 Installing and configuring the server

Setup overview

Your HP StorageWorks All-in-One Storage System comes preinstalled with the Windows® Storage Server™ 2003 R2 operating system. Windows Storage Server 2003 R2 extends the Windows Storage Server 2003 operating system, providing a more efficient way to manage and control access to local and remote resources. In addition, Windows Storage Server 2003 R2 provides a scalable, security-enhanced Web platform for simplified branch server management, improved identity and access management, and more efficient storage management.

Planning for installation

Before you install your HP StorageWorks All-in-One Storage System, you need to make a few decisions.

Determining a network access method

Before beginning setup and startup procedures, decide upon an access method to connect to the storage system. The type of network access you select is determined by whether or not the network has a Dynamic Host Configuration Protocol (DHCP) server. If the network has a DHCP server, you can access the storage system through the direct attachment, remote browser, Remote Desktop, or remote management methods. If your network does not have a DHCP server, you must access the storage system through the direct attachment method.

NOTE:

The direct attachment method requires a display, keyboard, and mouse.

Table 2 Network access methods

Access method	I.E. 5.5 or later required?	Storage system desktop accessible?	HP Rapid Startup Wizard access	Notes
Direct attachment	No	Yes	Directly from the storage system desktop.	Requires a monitor, mouse, and keyboard.
Remote browser	Yes	No	Directly from the HP StorageWorks All-in-One Storage System Management Console.	Does not display the storage system desktop.
Remote Desktop	No	Yes	Indirectly from the storage system desktop.	Windows Remote Desktop capability required on client.

Access method	I.E. 5.5 or later required?	Storage system desktop accessible?	HP Rapid Startup Wizard access	Notes
Remote management (Lights-Out 100 or Integrated Lights-Out 2)	Yes	Yes	Indirectly from the storage system desktop.	See the *HP ProLiant Lights-Out 100 Remote Management User Guide* or *HP Integrated Lights-Out 2 User Guide* for server access instructions.

NOTE:

The AiO400t Storage System does not include embedded Lights-Out 100 remote management support. This system requires the purchase and installation of the Lights-Out 100c Remote Management Card in order to use Lights-Out 100 remote management features. For more information about the Lights-Out 100c Remote Management Card, see http://h18004.www1.hp.com/products/servers/management/remotemgmt/lightsout100/index.html.

Planning a network configuration

Use the Rapid Startup Wizard to configure your storage system. This wizard displays automatically when you first start your system. Before you run the Rapid Startup Wizard, gather the network configuration information you need, including:

- User name and administrator password (the system provides you with defaults you need to change)
- E-mail addresses to set up system alerts
- SNMP settings
- Local area network (LAN) configuration settings

To help you gather this information, see "Configuring the server on the network" on page 30.

Configuration checklist

Use the following checklist to make sure you have completed all configuration tasks for your HP All-in-One Storage System. The steps for each task are explained in more detail in subsequent chapters of this guide.

Table 3 Installation and Configuration checklist

	Steps	Reference
☐	1. Unpack server, check kit contents, and become familiar with front and back panels of storage system. Locate and write down serial number of storage system.	See "Checking kit contents" on page 21.
☐	2. If you plan to rack the server, complete the rail installation instructions.	See the HP ProLiant rail installation instructions and tower-to-rack conversion instructions, if applicable.

☐	3. Connect cables; (optional) connect a keyboard, mouse, and monitor; power on server; and log on to the server.	See "Powering on the server" on page 22 and "Using the direct attach method" on page 23.
☐	4. Access the All-in-One Management Console.	See "Accessing the All-in-One Management Console" on page 23.
☐	5. Complete the storage system configuration worksheet.	See "Server configuration steps" on page 30.
☐	6. Run Rapid Startup Wizard.	See "Running the Rapid Startup Wizard" on page 32.
☐	7. Complete system configuration.	See "Completing system configuration" on page 32.
☐	8. Install the All-in-One Storage Manager Agent on network application servers.	See "Installing the All-in-One Storage Manager Agent" on page 33.
☐	9. Configure storage system for Web access, if necessary.	See "Configuring storage server for Web access (optional)" on page 181.

Installing the server

To install your HP StorageWorks All-in-One Storage System, follow the instructions in the sections below:

- Locating and writing down the serial number
- Checking kit contents
- Powering on the server

Locating and writing down the serial number

Before completing the installation portion of this guide, locate and write down the storage system's serial number, which you may need to access the All-in-One Storage Manager (ASM) later on during the set up process.

The All-in-One Storage System serial number is located in three places:

- Top of the server
- Back of the server
- Inside the server shipping box

Checking kit contents

Remove the contents, making sure you have all the components listed below. If components are missing, contact HP technical support.

- HP StorageWorks All-in-One Storage System (with operating system preloaded)
- Power cord(s)
- Product Documentation and Safety and Disposal Documentation CD
- *HP StorageWorks All-in-One Storage System Recovery DVD*
- *End User License Agreement*
- Certificate of Authenticity Card

NOTE:

Depending on your system, the following components might also be included:

- Bezel, bezel brackets, and screws
- Slide rail assembly
- Tower-to-rack conversion kit
- *HP ProLiant Essentials Integrated Lights-Out 2 Advanced Pack*
- *HP ProLiant Essentials Lights-Out 100i Advanced Pack*

Powering on the server

Power on the server after connecting the cables. For more information on your storage system model's hardware components, see "Server components" on page 35.

1. Power on the server by pushing the power button. The power LED illuminates green.
2. When the server powers on, an installation progress screen is displayed. The installation process takes approximately 10 to 15 minutes to complete and the server will reboot twice. No user interaction is required.

CAUTION:

Do not interrupt the installation process; when the installation sequence is complete, the system prompt appears.

3. See "Accessing the All-in-One Management Console" on page 23 to set up server access.

Factory image

The HP All-in-One Storage System is preconfigured with default storage settings and preinstalled with the Windows Storage Server 2003 R2 operating system (OS). This section provides additional details about the preconfigured storage.

Physical configuration

The DON'T ERASE logical disk supports the recovery process only and does not host a secondary operating system. If the operating system has a failure that might result from corrupt system files, a corrupt registry, or the system hangs during boot, see "System recovery" on page 121.

Data volumes are not carved at the factory or by the System Recovery DVD, and must be configured manually by the end user. Be sure to back up your user data, and then use the System Recovery DVD to restore the server to the factory default state as soon as conveniently possible.

Table 4 AiO Configurations

	Logical Disk 1	Logical Disk 2
• AiO400r • AiO400t	• Operating System Volume • RAID 5 • Physical Drives 1–4	• DON'T ERASE Volume • RAID 5 • Physical Drives 1–4

AiO600	• Operating System Volume • RAID 5 • Physical Drives 1–6	• DON'T ERASE Volume • RAID 5 • Physical Drives 1–6

Default boot sequence

The BIOS supports the following default boot sequence:

1. DVD-ROM
2. HDD
3. PXE (network boot)

Under normal circumstances, the storage system boots up from the OS logical drive.

- If the system experiences a drive failure, the drive displays an amber disk failure LED.
- If a single drive failure occurs, it is transparent to the OS.

Accessing the All-in-One Management Console

Before accessing the All-in-One Management Console, verify that the storage system is completely installed in the rack, and that all cables and cords are connected.

To access the All-in-One Management Console, you can use these access methods:

Direct attach	To connect directly to the storage system without using the network.
Remote browser	To establish a browser-based connection to the All-in-One Management Console from a remote client running Internet Explorer 5.5 (or later).
Remote Desktop	To establish a connection from a remote client without using a browser. This method requires the client to have Windows Remote Desktop capability.
Remote management	To establish a browser-based connection from a remote client using the HP Lights-Out 100 (LO100) or HP Integrated Lights-Out 2 (iLO 2) interface.

For more information, see "Planning for installation" on page 19.

IMPORTANT:

An IP address can be substituted for a storage system's serial number and hyphen when using either remote browser or Remote Desktop methods to access the All-in-One Management Console. For example: 192.0.0.1 can be substituted for TWT08466-.

Using the direct attach method

You can access the All-in-One Management Console using a monitor, mouse, and keyboard directly attached to the storage system.

To connect the storage system to a network using the direct attach method

1. Log on to the HP All-in-One Storage System with the default user name `administrator` and the password `hpinvent`.

   The HP All-in-One Storage System Management Console and Rapid Startup Wizard start automatically.

NOTE:

You can change the administrator name and password when you configure the server using the Rapid Startup Wizard. See "Running the Rapid Startup Wizard" on page 32.

2. To complete network configuration using the Rapid Startup Wizard, see "Configuring the server on the network" on page 30.

Using the remote browser method

The storage system ships with DHCP enabled on the network port. If the server is placed on a DHCP-enabled network and the serial number of the device is known, the server can be accessed through a client running Internet Explorer 5.5 (or later) on that network using the TCP/IP 3202 port.

IMPORTANT:

Before you begin this procedure, ensure that you have the following:

- Windows-based PC loaded with Internet Explorer 5.5 (or later) on the same local network as the storage system
- DHCP-enabled network
- Serial number or IP address of the storage system

To connect the server to a network using the remote browser method, you must first ensure that the client is configured to download signed ActiveX controls.

To enable ActiveX controls

1. On the remote client machine, open the Internet Explorer web browser and select **Tools > Internet Options > Security**.

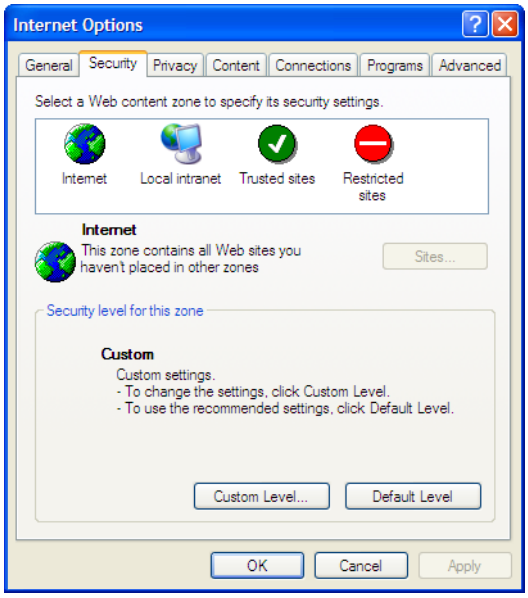
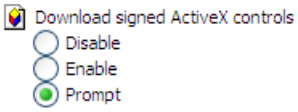


Figure 1 Internet options screen

2. On the Security screen, select **Internet** or **Local intranet** web content zone, then click **Custom Level**.
3. Scroll down to locate the **ActiveX Controls and plug-ins settings**.
4. At **Download signed ActiveX controls settings**, select **Enable** to enable ActiveX or **Prompt** to launch a notice requiring approval before ActiveX is enabled.



5. Click **OK** to close the **Security Settings** dialog box.
6. If prompted **Are you sure you want to change the security settings for this zone**, click **YES**.
7. On the **Internet Options** dialog box, click **OK** to finish.

To connect the storage system to a network using the remote browser method

1. On the remote client machine open Internet Explorer and enter `https://` and the serial number of the storage system followed by a hyphen (-), and then `:3202`. For example, `https://D4059ABC3433-:3202`. Press **Enter**.

NOTE:

If you are able to determine the IP address from your DHCP server, you can substitute the IP address for the serial number and hyphen (-). For example: `192.100.0.1:3202`.

2. Click **OK** on the **Security Alert** prompt.

3. Log on to the HP All-in-One Storage System with the default user name `administrator` and the password `hpinvent`.

NOTE:

You can change the administrator name and password when you configure the server using the "Running the Rapid Startup Wizard" on page 32.

4. To complete network configuration using the Rapid Startup Wizard, see "Configuring the server on the network" on page 30.

IMPORTANT:

If you are using the remote browser method to access the All-in-One Management Console and Rapid Startup Wizard, always close the remote session before closing your Internet browser. Closing the Internet browser does not close the remote session. Failure to close your remote session impacts the limited number of remote sessions allowed on the storage system at any given time.

Using the Remote Desktop method

Remote Desktop provides the ability for you to log onto and remotely administer your server, giving you a method of managing it from any client. Installed for remote administration, Remote Desktop allows only two concurrent sessions. Leaving a session running takes up one license and can affect other users. If two sessions are running, additional users will be denied access.

To connect the HP All-in-One Storage System to a network using the Remote Desktop method

1. On the PC client, select **Start > Run**. At **Open**, type `mstsc`, then click **OK**.
2. Enter the serial number of the storage system followed by a hyphen (-) in the **Computer** box and click **Connect**. For example: `D4059ABC3433-`.

NOTE:

If you are able to determine the IP address from your DHCP server, you can substitute the IP address for the serial number and hyphen (-). For example: `192.100.0.1`.

3. Log on to the HP All-in-One Storage System with the default user name `administrator` and the password `hpinvent`.

   The All-in-One Management Console and Rapid Startup Wizard start automatically.

NOTE:

You can change the administrator name and password when you configure the server using the "Running the Rapid Startup Wizard" on page 32.

4. To complete network configuration using the Rapid Startup Wizard, see "Configuring the server on the network" on page 30.

Logging off and disconnecting

Remote Desktop provides two options when closing a client: you can either disconnect or log off the system.

Disconnecting leaves the session running on the server. You can reconnect to the server and resume the session. If you are performing a task on the server, you can start the task and disconnect from the session. Later, you can log back on the server, re-enter the session, and either resume the task or check results. This is especially helpful when operating over a remote connection on a long-distance toll line.

Ending the session is known as *logging off*. Logging off ends the session running on the server. Any applications running within the session are closed, and unsaved changes made to open files will be lost. The next time you log onto the server, a new session is created.

Remote Desktop requires that all connecting users be authenticated, which is why users must log on each time they start a session.

Telnet Server

Telnet Server is a utility that lets users connect to machines, log on, and obtain a command prompt remotely. Telnet Server is preinstalled on the storage system, but must be activated before use.

△ CAUTION:

For security reasons, the Telnet Server is disabled by default. The service needs to be modified to enable access to the storage system with Telnet.

Enabling Telnet Server

The Telnet Server service needs to be enabled prior to its access. The service can be enabled by opening the services MMC:

1. Select **Start > Run**, and then enter **services.msc**.
2. Locate and right-click the Telnet service and then select **Properties**.
3. Choose one of the following:
   - For the Telnet service to start up automatically on every reboot, in the Startup Type drop-down box click **Automatic**, and then click **OK**.
   - For the Telnet service to be started manually on every reboot, in the Startup Type drop-down box click **Manual**, and then click **OK**.

On the storage system, access the command line interface either by Remote Desktop or a direct connection, and then enter the following command:

net start tlntsvr

Sessions information

The sessions screen provides the ability to view or terminate active sessions.

Using remote management methods

HP StorageWorks All-in-One Storage Systems provide remote management functionality through HP ProLiant Lights-Out technologies. The AiO400r Storage System includes a Lights-Out 100 (LO100) port with Advanced features. The AiO600 Storage System includes an Integrated Lights-Out 2 (iLO 2) port with Advanced features.

The AiO400t Storage System does not include embedded Lights-Out 100 remote management support. This system requires the purchase and installation of the Lights-Out 100c Remote Management Card in order to use Lights-Out 100 remote management features. For more information about the Lights-Out 100c Remote Management Card, see http://h18004.www1.hp.com/products/servers/management/remotemgmt/lightsout100/index.html.

For more information about HP ProLiant Lights-Out technologies, see http://h18013.www1.hp.com/products/servers/management/remotemgmt.html.

Using the Lights-Out 100 method

HP Lights-Out 100 allows you to remotely manage HP All-in-One Storage Systems remotely over an Ethernet connection. It provides embedded KVM over IP for full remote graphical console capabilities. This complements the virtual media and power control for complete entry level Lights-Out remote management. LO100 also enables anytime access to system management information such as hardware health and event logs.

For more information on using HP LO100, see the *HP ProLiant Lights-Out 100 Remote Management User Guide*.

To quickly set up LO100 using the default settings for LO100 Advanced features on AiO400r and AiO400t Storage Systems, follow these steps:

1. Ensure that a network cable is connected to the LO100 port located on the back of the storage system.

NOTE:

This connection method is easiest when the connection is to a DHCP and DNS supported network.

2. If you are using DHCP (IP addressing), you will need to input a static IP address by using the direct attach method and the IPMI section of the BIOS to read the DHCP address. If you are not using DHCP, use this procedure to set a static IP address.
3. Using the methods described in the *HP ProLiant Lights-Out 100 Remote Management User Guide*, connect to the LO100 port.

IMPORTANT:

Log on using the default LO100 user name `admin` and password `admin`.

4. If desired, you can change the default user name and password on the administrator account to your predefined selections.
5. Set up your user accounts, if using the local accounts feature.
6. Ensure that LO100 advanced features are activated. If they are not, activate these features by entering a license key from the included *HP ProLiant Essentials Lights-Out 100i Advanced Pack*.

7. Access the HP All-in-One Storage System using the LO100 Remote Console functionality. Log on to the HP All-in-One Storage System with the default user name `administrator` and the password `hpinvent`. The HP All-in-One Storage System Management Console starts automatically.

NOTE:

When the Remote Console feature is enabled, you can get access to the storage system's login screen.

The Lights-Out 100 port comes with factory default settings, which the administrator can change. See the *HP ProLiant Lights-Out 100 Remote Management User Guide* for information about changing these settings. To obtain this guide, go to http://www.hp.com/support/manuals, navigate to the servers section, and select **Server management**. In the ProLiant Essentials Software section, select **HP Lights-Out 100i (LO100i) Software**.

Using the Integrated Lights-Out 2 method

Integrated Lights-Out 2 (iLO 2) is HP's fourth generation of Lights-Out management technology that allows you to perform virtually any system administrator or maintenance task remotely as if you were using its keyboard, mouse and monitor, power button and floppy, CD or USB key, whether or not the server is operating. It is available on the AiO600 in two forms, iLO 2 Standard and iLO 2 Advanced. iLO 2 Standard provides basic system board management functions, diagnostics and essential Lights-Out functionality on supported storage systems. iLO 2 Advanced provides advanced remote administration functionality as a licensed option, which is included with the HP All-in-One Storage System.

The Integrated Lights-Out port on the storage system can be configured through the Rapid Startup Wizard or through the iLO 2 ROM-Based Setup Utility (RBSU). SNMP is enabled and the Insight Management Agents are preinstalled.

The HP iLO 2 management processor provides multiple ways to configure, update, operate, and manage servers remotely. The HP StorageWorks 600 All-in-One Storage System is preconfigured with iLO 2 default factory settings, including a default user account and password. These settings can be found on the iLO 2 Default Network Settings tag on the front of the server. If iLO 2 is connected to a network running DNS and DHCP, you can use it immediately without changing any settings.

For more information on using HP iLO 2, see the *HP Integrated Lights-Out 2 User Guide*.

To quickly set up iLO 2 using the default settings for iLO 2 Standard and iLO 2 Advanced features on AiO600 Storage System, follow these steps:

1. Ensure that a network cable is connected to the iLO 2 port located on the back of the storage system.

NOTE:

This connection method is easiest when the connection is to a DHCP and DNS supported network.

2. If not using dynamic DHCP (IP addressing), you will need to input a static IP address by using the direct attach method and the iLO 2 RBSU.

3. Using the methods described in the *HP Integrated Lights–Out 2 User Guide*, connect to the iLO 2 port.

NOTE:

To find the default iLO 2 log on settings, see the iLO 2 Default Network Settings card attached to your server. The default DNS, administrator name, and password needed to log on will be on this card.

4. If desired, you can change the default user name and password on the administrator account to your predefined selections.
5. Set up your user accounts, if using the local accounts feature.
6. Activate iLO 2 advanced features by entering a license key from the included *HP ProLiant Essentials Integrated Lights-Out 2 Advanced Pack*.
7. Access the HP All-in-One Storage System using the iLO 2 Remote Console functionality. Log on to the HP All-in-One Storage System with the default user name `administrator` and the password `hpinvent`. The All-in-One Management Console starts automatically.

NOTE:

When the Remote Console feature is enabled, you can get access to the storage system's login screen.

The Integrated Lights-Out 2 port comes with factory default settings, which the administrator can change. Administrators may want to add users, change SNMP trap destinations, or change networking settings. See the *HP Integrated Lights-Out 2 User Guide* for information about changing these settings. To obtain this guide, go to http://www.hp.com/support/manuals, navigate to the servers section, and select **Server management**. In the ProLiant Essentials Software section, select **HP Integrated Lights-Out 2 (iLO 2) Standard Firmware**.

Configuring the server on the network

Before you begin

When first powering on the storage system you need to have some configuration data readily available to complete the Running the Rapid Startup Wizard. Complete the Server configuration steps and use the data collected to initialize the storage system.

NOTE:

Ensure you are logged onto the HP All-in-One Storage System as a local or domain administrator.

Table 5 Server configuration steps

Configuration Steps
Administrative Identity

Configuration Steps	
User name	Change system administrator's user name, which is set by default to `administrator`.
User password	Change system administrator's password, which is set by default to `hpinvent`.
Alert E-mail Notification	
E-mail address alert sent to	E-mail address for critical, warning, or informational messages about server status.
E-mail address alert sent from	Must be a valid, well-formed e-mail address that will appear as the sender of server status e-mail alerts.
SMTP server name or IP address	Must be an e-mail server on your network that supports the Simple Mail Transfer Protocol (SMTP).
SNMP Settings (to be completed only if needed)	
Contact person	System administrator for the storage system. The contact and location will be provided to any SNMP management computer that requests them.
System location	Any text string, such as a location or phone number. For example, `Floor #3, Financial Services Bldg.`
Community name No. 1	The community name is used for network authentication when sending outgoing SNMP messages.
Trap destination No. 1	The IP address of a management computer that will receive SNMP messages from the storage system using the above community name.
Community name No. 2	Same as above.
Trap destination No. 2	Same as above.
Network Interfaces (to be completed for non-DHCP configurations)	
Local area connection 1	A local area connection is automatically created for each network adapter that is detected.
IP address	An Internet Protocol (IP) address is assigned to the server. If it is not automatically assigned, enter the IP address that you want to assign to this server.
Subnet mask	A mask is used to determine what subnet an IP address belongs to.
Default gateway	The gateway in a network that the network adapter will use to access all other networks.
Local area connection 2	Any additional local area connections can be renamed to prevent confusion.
IP address	Same as above.
Subnet mask	Same as above.
Default gateway	Same as above.

Configuration Steps	
iLO 2 settings	Change the host name, IP settings, and administrator settings.
DNS server	A Domain Name System (DNS) server name is required to provide for domain name to IP address resolution.
WINS server	A Windows Internet Naming Service (WINS) server name is required to determine the IP address associated with a particular network computer.
Server Name	
Server name	Assign a unique name to the storage system. This name identifies the storage system on the network.

Running the Rapid Startup Wizard

The Rapid Startup Wizard is only displayed during the initial setup process. This wizard guides you through configuring the following system settings:

- Date, time, and time zone
- Administrator identity (user name and password)
- Alert e-mail notification
- Lights-Out 100 (LO100) / Integrated Lights-Out 2 (iLO 2) settings
- Simple Network Management Protocol (SNMP) settings
- Network interfaces
- Server name

For more information about the configuration settings available in the Rapid Startup Wizard, click **Help** to see the corresponding Rapid Startup Wizard online help topic.

Completing system configuration

After the storage system is physically set up and the basic configuration is established, you must complete additional setup tasks. Depending on the deployment scenario of the storage system, these steps can vary. These additional steps can include:

- Running Microsoft Windows Update—HP highly recommends that you run Microsoft Windows updates to identify, review, and install the latest, applicable, critical security updates on the storage system.
- Creating and managing users and groups—User and group information and permissions determine whether a user can access files. If the storage system is deployed into a workgroup environment, this user and group information is stored locally on the device. By contrast, if the storage system is deployed into a domain environment, user and group information is stored on the domain.
- Joining workgroup and domains—These are the two system environments for users and groups. Because users and groups in a domain environment are managed through standard Windows or Active Directory domain administration methods, this document discusses only local users and groups, which are stored and managed on the storage system. For information on managing users and groups on a domain, see the domain documentation available on the Microsoft web site.
- Using Ethernet NIC teaming (optional)—Select models are equipped with an HP or Broadcom NIC Teaming utility. The utility allows administrators to configure and monitor Ethernet network

interface controller (NIC) teams in a Windows-based operating system. These teams provide options for increasing fault tolerance and throughput.

- Activating iLO 2 Advanced features using a license key—The Remote Console feature of iLO 2 requires a license key. The key is included with the storage system inside the Country Kit. See the iLO 2 Advanced License Pack for activation instructions.
- Adjusting logging for system, application, and security events.
- Installing third-party software applications—For example, these might include an antivirus application that you install.
- Registering the system — To register the system, refer to the HP Registration website (http://register.hp.com).

Installing the All-in-One Storage Manager Agent

If you plan to perform data migration tasks for any application servers on your network using the wizards that are available in the All-in-One Storage Manager, you must first install the All-in-One Storage Manager Agent on those application servers. Follow these instructions before performing any data migration operations.

Installing the All-in-One Storage Manager Agent on network application servers

To install the All-in-One Storage Manager Agent on a network application server:

1. Locate the file at `c:\\hpnas\components\allinonestoragemanager\agent`.
2. Copy the file to the application server(s) you will use to perform data migration tasks.
3. Run the copied file on each application server to install the All-in-One Storage Manager Agent.

or

1. On the application server that stores data to be migrated, insert the *HP StorageWorks All-in-One Storage System Recovery DVD.*

NOTE:

If the application server is in a remote location, use Remote Desktop Connection to access the server, copy the Agent installation files, and run the Agent installation.

2. Navigate to the \All-in-One Storage Manage\Agent folder on the DVD.
3. Double-click **asmagentinstaller.exe.**
4. Follow the on-screen installation instructions.

After completing the All-in-One Storage Manger Agent installation on the application servers, you can then schedule data migration using the HP All-in-One Storage System wizards.

2 Storage system components

This chapter provides illustrations of the AiO400r, AiO400t, and AiO600 Storage System hardware components.

NOTE:

Connecting the storage system power cord illuminates the LEDs on the front of the unit, the Systems Insight Display LED (if applicable), and the LEDs on the NIC connector (rear panel). The Lights-Out NIC LED (rear panel) illuminates if the Lights-Out port is connected. Connecting the power cord also restores the storage server to whatever previous powered state it was last in. This could result in the server powering up, the fans operating, and the power indicator coming on.

NOTE:

The keyboard, mouse, and monitor are used only for the direct attach method of accessing the system. They are not provided with your storage system.

HP StorageWorks 400r All-in-One Storage System

The following figures show components, controls and indicators located on the front and rear panels of the AiO400r.

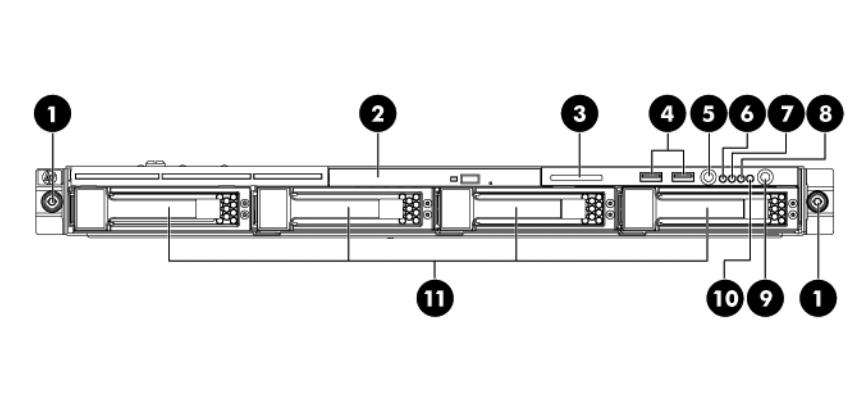


Figure 2 HP StorageWorks 400r All-in-One Storage System front panel

Table 6 HP StorageWorks 400r All-in-One Storage System front panel components

Item	Description	Status
1	Thumbscrews for rack mounting	N/A
2	DVD ROM drive	N/A

Item	Description	Status
3	Serial number pull tab	N/A
4	USB 2.0 ports	N/A
5	Unit identification (UID) LED button	Blue = Activated Off = Deactivated
6	System health LED	Green = Normal (system on) Flashing amber = System health degraded Flashing red = System health critical Off = Normal (system off)
7	NIC 1 activity LED	Green = Network link Flashing = Network link and activity Off = No network connection
8	NIC 2 activity LED	Green = Network link Flashing = Network link and activity Off = No network connection
9	Power button	Green = System on Amber = System off
10	HDD LED	Green = HDD install ready Flashing green = Data access Off = No access
11	Hard disk drive (HDD) bays 1, 2, 3, and 4	See "SAS and SATA hard drive LED combinations" on page 43 for HDD LED status descriptions.

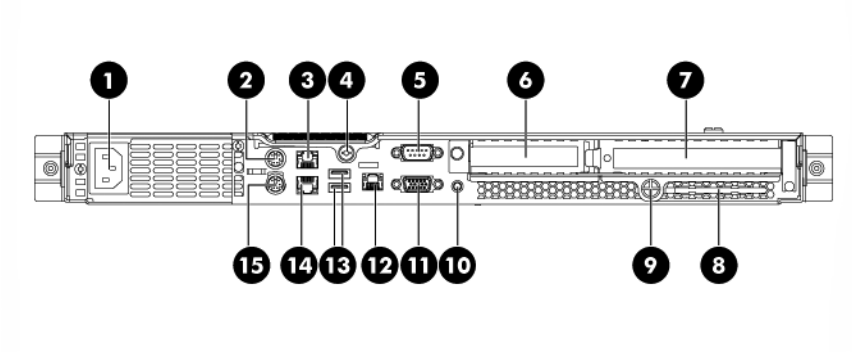


Figure 3 HP StorageWorks 400r All-in-One Storage system rear panel

Table 7 HP StorageWorks 400r All-in-One Storage System rear panel components

Item	Description	Status / Description
1	Power supply cable socket	N/A
2	PS/2 mouse port (green)	N/A

Item	Description	Status / Description
3	GbE LAN port for NIC 2	Green = 10/100 Mbps connection Orange = 1000 Mbps connection
4	Captive thumbscrew for top cover	N/A
5	Serial port	N/A
6	Low profile/Half length expansion slot	N/A
7	Full height/Full length expansion slot	Populated with HP Smart Array E200 controller
8	T10/T15 Wrench	N/A
9	Thumbscrew for PCI cage	N/A
10	UID LED button	Blue = Activated Off = Deactivated
11	VGA port	N/A
12	HP LO100i Management LAN Port	Blinking green = Ongoing network activity Green = Existing network link
13	USB 2.0 ports	N/A
14	GbE LAN port for NIC 1/Management	Green = 10/100 Mbps connection Orange = 1000 Mbps connection
15	PS/2 keyboard port (purple)	N/A

HP StorageWorks 400t All-in-One Storage System

The following figures show components, controls, and indicators located on the front and rear panels of the AiO400t storage system.

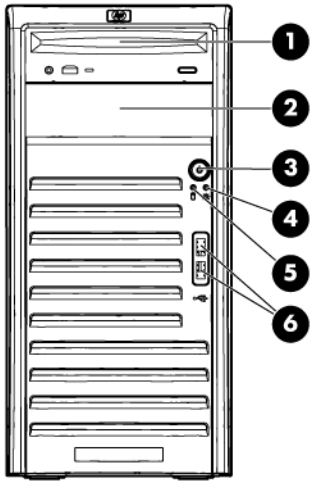


Figure 4 AiO400t front panel (bezel on)

Table 8 AiO400t front panel components (bezel on)

Item	Description	Status
1	DVD ROM drive	N/A
2	2nd removable media drive bay cover	N/A
3	Power button	N/A
4	System power	Green = Power on mode Amber = Standby mode
5	HDD activity	Green = Ongoing HDD activity
6	USB 2.0 ports	N/A

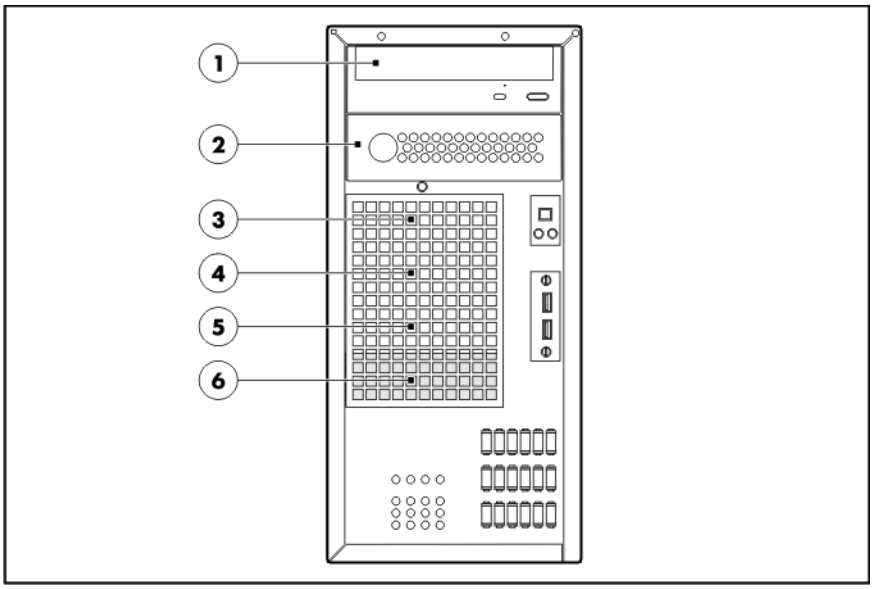


Figure 5 AiO400t front panel (bezel off)

Table 9 AiO400t front panel components (bezel off)

Item	Description
1	DVD ROM drive
2	2nd removable media drive bay EMI shield
3 — 6	Hard disk drives 1–4 behind EMI shield

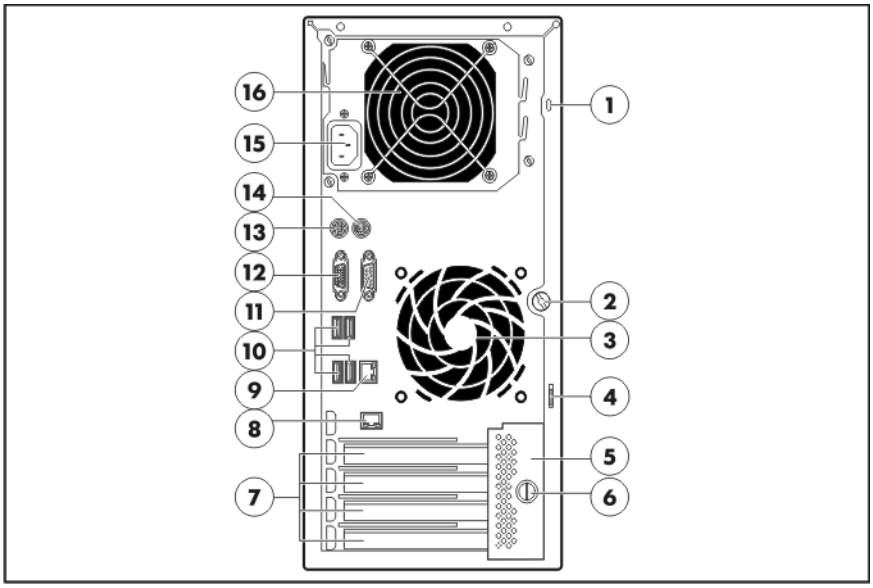


Figure 6 AiO400t rear panel

Table 10 AiO400t rear panel components

Item	Description	Status / Description
1	Kensington lock notch	N/A

Item	Description	Status / Description
2	Access panel thumbscrew	N/A
3	System fan	N/A
4	Cable lock provision notch	N/A
5	PCI slot cover retainer	N/A
6	PCI slot cover retainer thumbscrew	N/A
7	PCI slot covers	One slot populated with HP Smart Array E200 controller
8	Lights-Out remote management port (optional)	Management NIC activity and link Blinking green = Ongoing network activity Green = Existing network link
9	Embedded NIC port (RJ-45)	Embedded NIC link and activity Orange = 10/100 Mbps connection Green = GbE link connection Blinking yellow = Ongoing network activity
10	USB 2.0 ports	N/A
11	Serial port	N/A
12	Video port	N/A
13	PS/2 keyboard port	N/A
14	PS/2 mouse port	N/A
15	Power supply cable socket	N/A
16	PSU fan	N/A

HP StorageWorks 600 All-in-One Storage System

The following figures show components, controls, and indicators located on the front and rear panels of the AiO600.

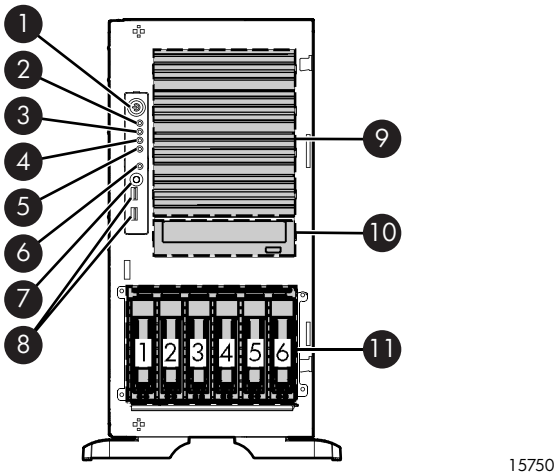


Figure 7 HP StorageWorks 600 All-in-One Storage System front panel

Table 11 HP StorageWorks 600 All-in-One front panel components

Item	Description	Status
1	Power on/Standby button	N/A
2	Power LED	Green = Power on Amber = System shut down, but power still applied Off = No power
3	Internal health LED	Green = Normal Amber = System health is degraded Red = System health is critical Off = Normal (when in standby mode)
4	External health LED (power supply)	Green = Normal Amber = Power redundancy failure Red = Critical power supply failure
5	NIC 1 activity LED	Green = Network link Flashing = Network link and activity Off = No network connection
6	UID LED	Blue = Activated Flashing = System remotely managed Off = Deactivated
7	UID button	N/A
8	USB connectors (2)	N/A
9	Removable media bays (4)	N/A
10	DVD+R/RW drive	N/A
11	Hot-plug hard drive bays	See "SAS and SATA hard drive LED combinations" on page 43 for HDD LED status descriptions.

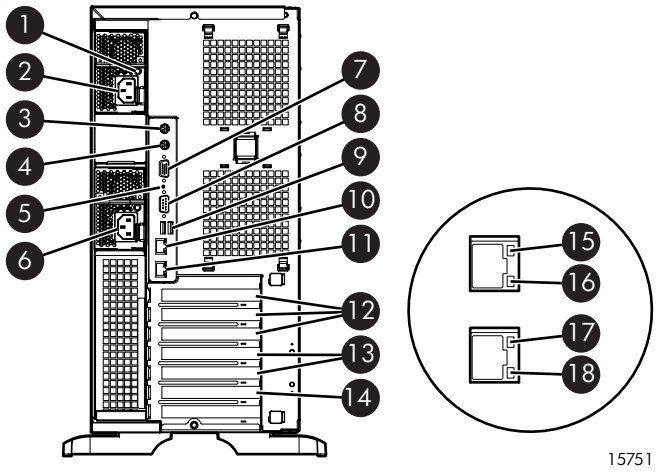


Figure 8 HP StorageWorks 600 All-in-One Storage System rear panel

Table 12 HP StorageWorks 600 All-in-One Storage System rear panel components

Item	Description	Status
1	Power Supply LED	Green = Power supply is on and functioning Off = No power or inadequate power supply
2	Power cord connector	N/A
3	Keyboard connector	N/A
4	Mouse connector	N/A
5	UID LED and button	Blue = Activated Flashing blue = Remote inquiry Off = Deactivated
6	Power cord connector	N/A
7	Video connector	N/A
8	Serial connector	N/A
9	USB connectors (2)	N/A
10	RJ-45 Ethernet connector (iLO 2 management)	N/A
11	RJ-45 Ethernet connector (data)	N/A
12	PCI Express x* slots (x4 routed)	N/A
13	PCI-X slots (100–MHz)	N/A
14	PCI-X slot (133–MHz)	N/A
15	iLO 2/data activity LED	Green or flashing = Network activity Off = No network activity
16	iLO 2/data link LED	Green = Linked to network

Item	Description	Status
		Off = Not linked to network
17	10/100/1000 NIC activity LED	Green or flashing = Network activity Off = No network activity
18	10/100/1000 NIC link LED	Green = Linked to network Off = Not linked to network

SAS and SATA hard drive LEDs

The following figure shows SAS/SATA hard drive LEDs. These LEDs are located on all HP All-in-One hot plug hard drives.

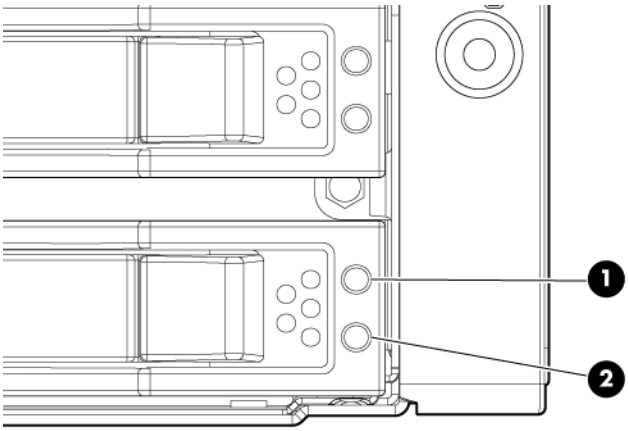


Figure 9 SAS/SATA hard drive LEDs

Table 13 SAS and SATA hard drive LED combinations

1. Fault/UID LED (amber/blue)	2. Online/activity LED (green)	Status
Alternating amber and blue	On, off, or flashing	The drive has failed, or a predictive failure alert has been received for this drive; it also has been selected by a management application.
Steadily blue	On, off, or flashing	The drive is operating normally, and it has been selected by a management application.
Amber, flashing regularly (1 Hz)	On	A predictive failure alert has been received for this drive. Replace the drive as soon as possible.
Off	On	The drive is online, but it is not active currently.
Amber, flashing regularly (1 Hz)	Flashing regularly (1 Hz)	**Do not remove the drive. Removing a drive may terminate the current operation and cause data loss.** The drive is part of an array that is undergoing capacity expansion or stripe migration, but a predictive failure alert has been received for this

1. Fault/UID LED (amber/blue)	2. Online/activity LED (green)	Status
		drive. To minimize the risk of data loss, do not replace the drive until the expansion or migration is complete.
Off	Flashing regularly (1 Hz)	**Do not remove the drive. Removing a drive may terminate the current operation and cause data loss.** The drive is rebuilding, or it is part of an array that is undergoing capacity expansion or stripe migration.
Amber, flashing regularly (1 Hz)	Flashing irregularly	The drive is active, but a predictive failure alert has been received for this drive. Replace the drive as soon as possible.
Off	Flashing irregularly	The drive is active, and it is operating normally.
Steadily amber	Off	A critical fault condition has been identified for this drive, and the controller has placed it offline. Replace the drive as soon as possible.
Amber, flashing regularly (1 Hz)	Off	A predictive failure alert has been received for this drive. Replace the drive as soon as possible.
Off	Off	The drive is offline, a spare, or not configured as part of an array.

3 Storage management overview

This chapter provides an overview of some of the components that make up the storage structure of the HP All-in-One Storage System.

Storage management elements

Storage is divided into four major divisions:

- Physical storage elements
- Logical storage elements
- File system elements
- File sharing elements

Each of these elements is composed of the previous level's elements.

Storage process management example

Figure 10 depicts many of the storage elements that one would find on a storage device. The following sections provide an overview of the storage elements.

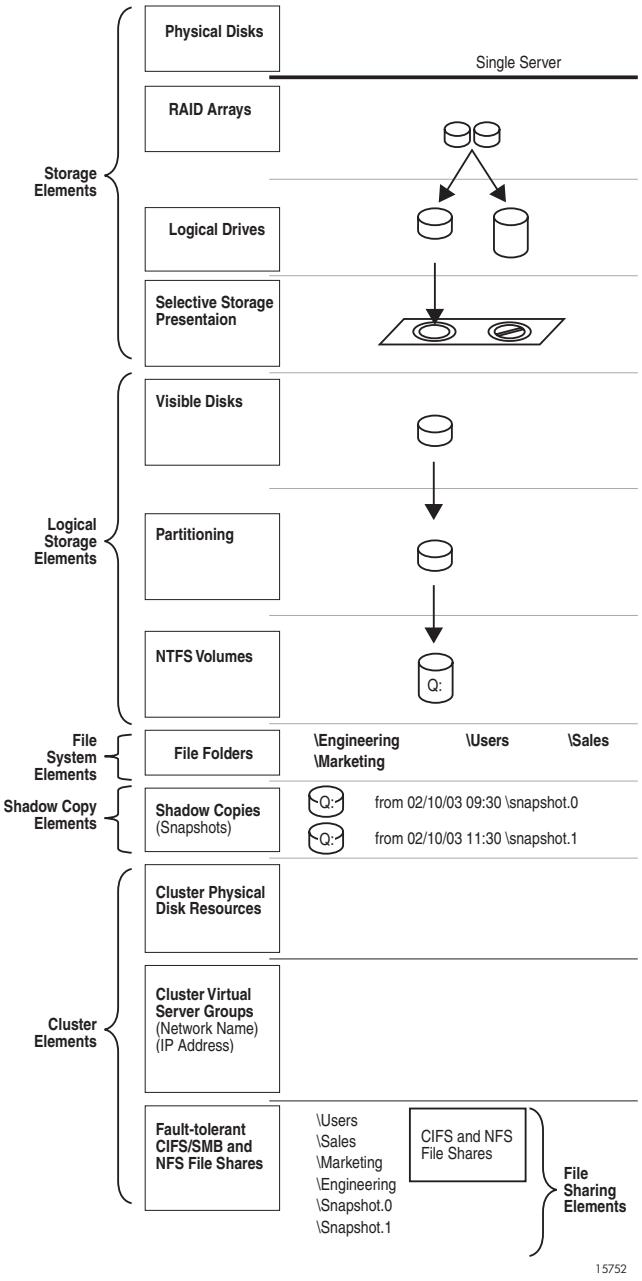


Figure 10 Storage process management example

Physical storage elements

The lowest level of storage management occurs at the physical drive level. Minimally, choosing the best disk carving strategy includes the following policies:

- Analyze current corporate and departmental structure.
- Analyze the current file server structure and environment.
- Plan properly to ensure the best configuration and use of storage.
  - Determine the desired priority of fault tolerance, performance, and storage capacity.
  - Use the determined priority of system characteristics to determine the optimal striping policy and RAID level.

- Include the appropriate number of physical drives in the arrays to create logical storage elements of desired sizes.

Arrays

See Figure 11. With an array controller installed in the system, the capacity of several physical drives (P1–P3) can be logically combined into one or more logical units (L1) called arrays. When this is done, the read/write heads of all the constituent physical drives are active simultaneously, dramatically reducing the overall time required for data transfer.

NOTE:

Depending on the storage system model, array configuration may not be possible or necessary.

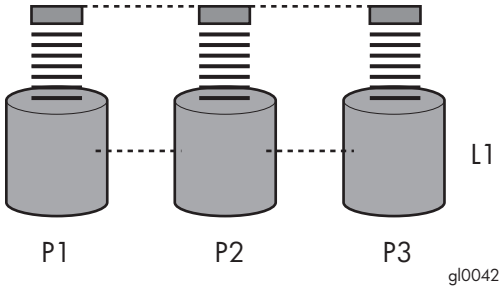


Figure 11 Configuring arrays from physical drives

Because the read/write heads are simultaneously active, the same amount of data is written to each drive during any given time interval. Each unit of data is termed a block. The blocks form a set of data stripes over all the hard drives in an array, as shown in Figure 12.

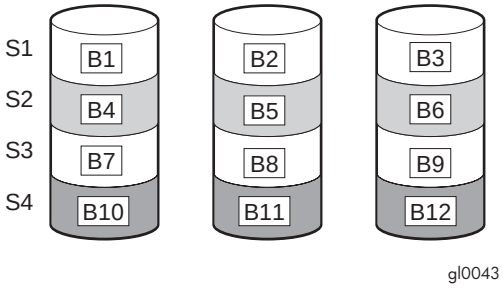


Figure 12 RAID 0 (data striping) (S1-S4) of data blocks (B1-B12)

For data in the array to be readable, the data block sequence within each stripe must be the same. This sequencing process is performed by the array controller, which sends the data blocks to the drive write heads in the correct order.

A natural consequence of the striping process is that each hard drive in a given array contains the same number of data blocks.

NOTE:

If one hard drive has a larger capacity than other hard drives in the same array, the extra capacity is wasted because it cannot be used by the array.

Fault tolerance

Drive failure, although rare, is potentially catastrophic. For example, using simple striping as shown in Figure 12, failure of any hard drive leads to failure of all logical drives in the same array, and hence to data loss.

To protect against data loss from hard drive failure, storage systems should be configured with fault tolerance. HP recommends adhering to RAID 5 configurations.

The table below summarizes the important features of the different kinds of RAID supported by the Smart Array controllers. The decision chart in the following table can help determine which option is best for different situations.

Table 14 Summary of RAID methods

	RAID 0 Striping (no fault tolerance)	RAID 1+0 Mirroring	RAID 5 Distributed Data Guarding	RAID 6 ADG
Maximum number of hard drives	N/A	N/A	14	Storage system dependent
Tolerant of single hard drive failure?	No	Yes	Yes	Yes
Tolerant of multiple simultaneous hard drive failures?	No	If the failed drives are not mirrored to each other	No	Yes (two drives can fail)

Online Spares

Further protection against data loss can be achieved by assigning an online spare (or hot spare) to any configuration except RAID 0. This hard drive contains no data and is contained within the same storage subsystem as the other drives in the array. When a hard drive in the array fails, the controller can then automatically rebuild information that was originally on the failed drive onto the online spare. This quickly restores the system to full RAID level fault tolerance protection. If using RAID Advanced Data Guarding (ADG) the system is able to have two drive failures simultaneously; however, if the third drive fails during this procedure, data will be lost.

Logical storage elements

Logical storage elements consist of those components that translate the physical storage elements to file system elements. The storage system uses the Window Disk Management utility to manage the various types of disks presented to the file system. There are two types of LUN presentation: basic disk and dynamic disk. Each of these types of disk has special features that enable different types of management.

Logical drives (LUNs)

While an array is a physical grouping of hard drives, a logical drive consists of components that translate physical storage elements into file system elements.

It is important to note that a LUN may extend over (span) all physical drives within a storage controller subsystem, but cannot span multiple storage controller subsystems.

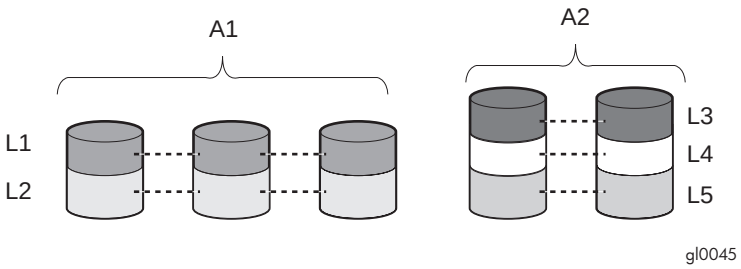


Figure 13 Two arrays (A1, A2) and five logical drives (L1 through L5) spread over five physical drives

NOTE:

This type of configuration may not apply to all storage systems and serves only as an example.

Through the use of basic disks, primary partitions or extended partitions can be created. Partitions can only encompass one LUN. Through the use of dynamic disks, volumes can be created that span multiple LUNs. The Windows Disk Management utility can be used to convert disks to dynamic and back to basic, and manage the volumes residing on dynamic disks. Other options include the ability to delete, extend, mirror, and repair these elements.

Partitions

Partitions exist as either primary partitions or extended partitions and can be composed of only one basic disk no larger than 2 TB. Basic disks can also only contain up to four primary partitions, or three primary partitions and one extended partition. In addition, the partitions on them cannot be extended beyond the limits of a single LUN. Extended partitions allow the user to create multiple logical drives. These partitions or logical disks can be assigned drive letters or be used as mount points on existing disks. If mount points are used, it should be noted that Services for UNIX (SFU) does not support mount points at this time. The use of mount points in conjunction with NFS shares is not supported.

Volumes

When planning dynamic disks and volumes, there is a limit to the amount of growth a single volume can undergo. Volumes are limited in size and can have no more than 32 separate LUNs, with each LUN not exceeding 2 terabytes (TB), and volumes totaling no more than 64 TB of disk space.

The RAID level of the LUNs included in a volume must be considered. All of the units that make up a volume should have the same high-availability characteristics. In other words, the units should all be of the same RAID level. For example, it would not be a good practice to include both a RAID 1+0 and a RAID 5 array in the same volume set. By keeping all the units the same, the entire volume retains the same performance and high-availability characteristics, making managing and maintaining the volume much easier. If a dynamic disk goes offline, the entire volume dependent on the one or more dynamic disks is unavailable. There could be a potential for data loss depending on the nature of the failed LUN.

Volumes are created out of the dynamic disks, and can be expanded on the fly to extend over multiple dynamic disks if they are spanned volumes. However, after a type of volume is selected, it cannot be altered. For example, a spanning volume cannot be altered to a mirrored volume without deleting and recreating the volume, unless it is a simple volume. Simple volumes can be mirrored or converted to spanned volumes. Fault-tolerant disks cannot be extended. Therefore, selection of the volume type

is important. The same performance characteristics on numbers of reads and writes apply when using fault-tolerant configurations, as is the case with controller-based RAID. These volumes can also be assigned drive letters or be mounted as mount points off existing drive letters.

The administrator should carefully consider how the volumes will be carved up and what groups or applications will be using them. For example, putting several storage-intensive applications or groups into the same dynamic disk set would not be efficient. These applications or groups would be better served by being divided up into separate dynamic disks, which could then grow as their space requirements increased, within the allowable growth limits.

NOTE:

We recommend that you allow All-in-One Storage Manager to allocate your storage. Dynamic disks are not supported by All-in-One Storage Manager.

File system elements

File system elements are composed of the folders and subfolders that are created under each logical storage element (partitions, logical disks, and volumes). Folders are used to further subdivide the available file system, providing another level of granularity for management of the information space. Each of these folders can contain separate permissions and share names that can be used for network access. Folders can be created for individual users, groups, projects, and so on.

File sharing elements

The storage system supports several file sharing protocols, including Distributed File System (DFS), Network File System (NFS), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Microsoft Server Message Block (SMB). On each folder or logical storage element, different file sharing protocols can be enabled using specific network names for access across a network to a variety of clients. Permissions can then be granted to those shares based on users or groups of users in each of the file sharing protocols.

Volume Shadow Copy Service overview

The Volume Shadow Copy Service (VSS) provides an infrastructure for creating point-in-time snapshots (shadow copies) of volumes. VSS supports 64 shadow copies per volume.

Shadow Copies of Shared Folders resides within this infrastructure, and helps alleviate data loss by creating shadow copies of files or folders that are stored on network file shares at pre-determined time intervals. In essence, a shadow copy is a previous version of the file or folder at a specific point in time.

By using shadow copies, a storage system can maintain a set of previous versions of all files on the selected volumes. End users access the file or folder by using a separate client add-on program, which enables them to view the file in Windows Explorer.

Shadow copies should not replace the current backup, archive, or business recovery system, but they can help to simplify restore procedures. For example, shadow copies cannot protect against data loss due to media failures; however, recovering data from shadow copies can reduce the number of times needed to restore data from tape.

Using storage elements

The last step in creating the element is determining its drive letter or mount point and formatting the element. Each element created can exist as a drive letter, assuming one is available and/or as mount points off of an existing folder or drive letter. Either method is supported. However, mount points can not be used for shares that will be shared using Microsoft Network File Services. They can be set up with both but the use of the mount point in conjunction with NFS shares causes instability with the NFS shares.

Formats consist of NTFS, FAT32, and FAT. All three types can be used on the storage system. However, VSS can only use volumes that are NTFS formatted. Also, quota management is possible only on NTFS.

Network adapter teaming

Network adapter teaming is software-based technology used to increase a server's network availability and performance. Teaming enables the logical grouping of physical adapters in the same server (regardless of whether they are embedded devices or Peripheral Component Interconnect (PCI) adapters) into a virtual adapter. This virtual adapter is seen by the network and server-resident network-aware applications as a single network connection.

Management tools

HP Systems Insight Manager

HP SIM is a web-based application that allows system administrators to accomplish normal administrative tasks from any remote location, using a web browser. HP SIM provides device management capabilities that consolidate and integrate management data from HP and third-party devices.

IMPORTANT:

You must install and use HP SIM to benefit from the Pre-Failure Warranty for processors, SAS and SCSI hard drives, and memory modules.

For additional information, refer to the Management CD in the HP ProLiant Essentials Foundation Pack or the HP SIM website (http://www.hp.com/go/hpsim).

Management Agents

Management Agents provide the information to enable fault, performance, and configuration management. The agents allow easy manageability of the server through HP SIM software, and thirdparty SNMP management platforms. Management Agents are installed with every SmartStart assisted installation or can be installed through the HP PSP. The Systems Management homepage provides status and direct access to in-depth subsystem information by accessing data reported through the Management Agents. For additional information, refer to the Management CD in the HP ProLiant Essentials Foundation Pack or the HP website (http://www.hp.com/servers/manage).

All-in-One Storage Manager

HP StorageWorks All-in-One Storage Manager (ASM) is a storage hosting and management tool that radically simplifies:

- Hosting storage for applications and shared folders, page 61
- Data protection, page 81
- Managing storage, page 89
- Monitoring storage, page 93

ASM provides storage-allocation wizards that walk you through the process of allocating and configuring storage on your HP All-in-One Storage System to host application data and shared folders. The storage-allocation wizards also allow you to schedule backups and snapshots of hosted application data and shared folders.

Other wizards are provided to help you set up SQL Server database storage, storage for user-defined applications, and storage for shared folders.

ASM is designed to work seamlessly with Windows administrator tools, the HP All-in-One Storage System Management application, Microsoft iSCSI Target, and Data Protector Express. For example, you can change your HP All-in-One Storage System's:

- Storage allocations (quotas), shared folder permissions and names, and snapshot schedules using ASM, Windows administrator tools, and the HP All-in-One Storage System Management applications.
- Media rotation type using ASM and Data Protector Express.

However, you should not use Windows administrator tools to change the paths to storage configured on your HP All-in-One Storage System or file directories created by ASM on application servers with storage hosted on your HP All-in-One Storage System. Doing so will break the iSCSI communication paths between your application servers and HP All-in-One Storage System, and make it so ASM can no longer locate allocated storage areas on your HP All-in-One Storage System.

Software requirements

ASM comes preinstalled on your HP All-in-One Storage System. A license key is not required for ASM.

Software support

Only storage for application servers running on Windows Server 2003 and on the same domain as your HP All-in-One Storage System can be hosted.

ASM provides storage-management services for the following applications:

Table 15 Software support

Microsoft Exchange Server 2003 and 2007	See "Using the Host an Exchange Storage Group Wizard" on page 62.
File sharing services on local storage	See "Using the Create a Shared Folder Wizard" on page 64.
Microsoft SQL Server 2000 and 2005	See "Using the Host a SQL Server Database Wizard" on page 65.
User-defined applications	See "Using the Host a User-Defined Application Wizard" on page 67.

Microsoft iSCSI Target and Data Protector Express are required to host application storage and create backups using ASM. Microsoft iSCSI Target and Data Protector Express come preinstalled on your HP All-in-One Storage System. A license key is not required for Microsoft iSCSI Target. Your license key for Data Protector Express comes preinstalled on your HP All-in-One Storage System.

Storage management infrastructure

The purpose of ASM is to simplify storage management, so that you do not need to understand the complexities of allocating and configuring storage, and hosting application storage on your HP All-in-One Storage System. ASM handles two types of use models:

- Managing storage for application servers, page 53
- Managing storage for shared folders, page 54

Managing storage for application servers

With ASM, you can allocate, configure, and host storage for applications residing on servers that host Exchange, SQL Server, and user-defined applications using the Host an Exchange Storage Group Wizard, Host a SQL Server Database Wizard, and Host a User-Defined Application Wizard.

The wizards suggest a default storage size, plus default advanced configuration settings, such as RAID level, for each application component. You can customize all the defaults to fit your storage needs. However, the default advanced settings provided for Exchange and SQL Server are based on HP storage, Exchange, and SQL Server best practices and should generally not be changed.

For application storage, ASM creates an iSCSI LUN on your HP All-in-One Storage System for each storage group component, database component, or the user-defined application you select to host in the storage-allocation wizard, and exports it to the application server whose storage will be hosted. ASM also creates a LUN on your HP All-in-One Storage System to host the storage group component, database component, or the user-defined application you selected in the storage-allocation wizard. All storage communication passes through the iSCSI LUN on the application server to the LUN on your HP All-in-One Storage System. This allows data saved by the application to the iSCSI LUN on the application server to be automatically saved to your HP All-in-One Storage System instead (see Figure 14).

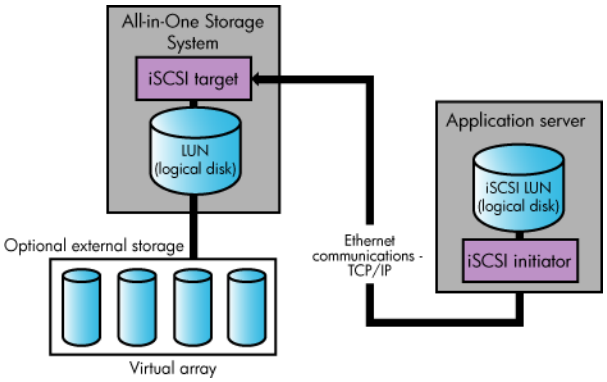


Figure 14 Application storage infrastructure

NOTE:

The iSCSI communication path is transparent to the application, application server, and Windows Explorer. The application, application server, and Windows Explorer believe the data is stored on the application server. So, to view the application data, you must navigate to the iSCSI LUN(s) on the application server, not the LUN(s) on your HP All-in-One Storage System, using Windows Explorer.

ASM provides automated data migration for Exchange and SQL Server. ASM discovers Exchange storage group and SQL Server database components and hosts the storage components you select through the storage-allocation wizards. ASM automatically migrates the data for the selected storage components to your HP All-in-One Storage System. ASM also configures the application to read and write data for the hosted storage component to the iSCSI LUNs created on the application server by ASM.

ASM does not provide automated data migration for user-defined application servers. You must manually migrate the application data to your HP All-in-One Storage System after using the Host a User-Defined Application Wizard to allocate and configure storage space. See "Migrating user-defined application data from a remote application" on page 80 for more information. You must also configure the application to read and write data to the iSCSI LUN created on the application server by ASM. See the application's documentation for more information.

Managing storage for shared folders

With ASM, you can set up and monitor top-level shared folders (file shares) using the Create a Shared Folder Wizard. The wizard suggests a default storage size for each shared folder, plus default advanced configuration settings, such as RAID level. You can customize all the defaults to fit your storage needs.

For shared folder storage, ASM creates a LUN on your HP All-in-One Storage System to hold the shared folder and then creates the shared folder (see Figure 15). Shared folders whose storage is configured with the same RAID level are created on the same LUN.

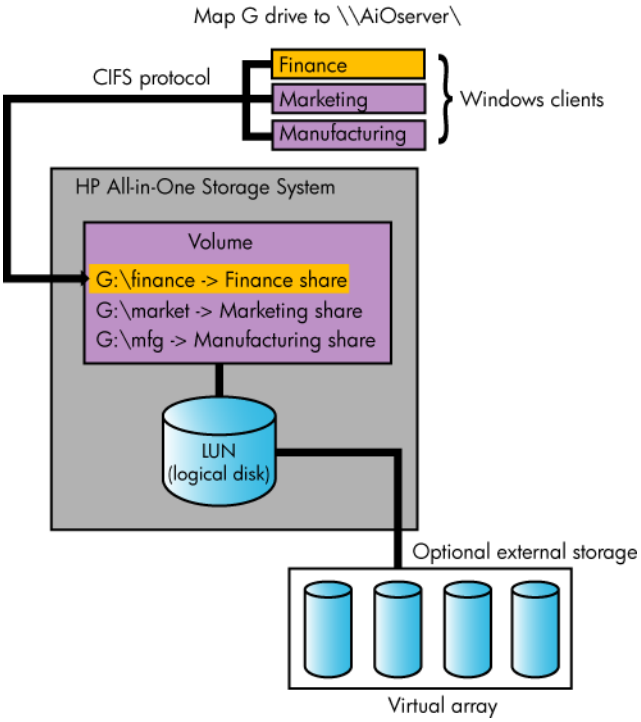


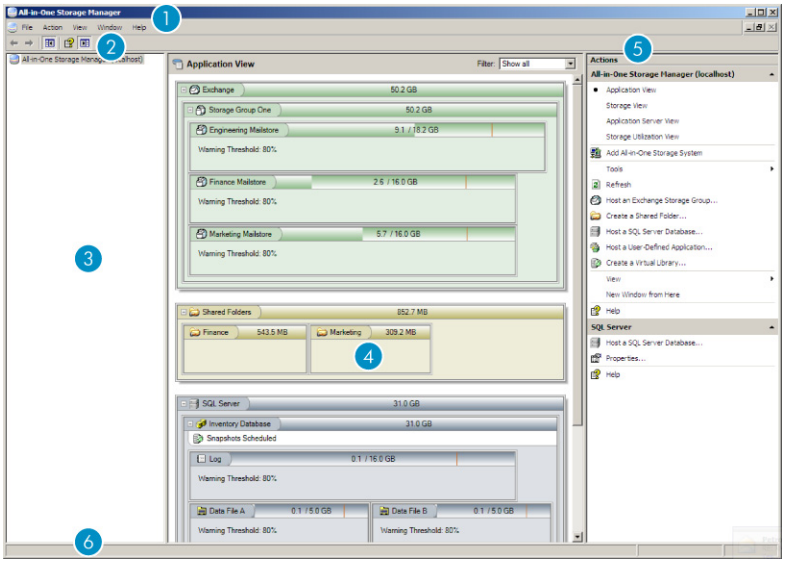
Figure 15 Shared folder storage infrastructure

ASM discovers any top-level and nested shared folders on your HP All-in-One Storage System during setup and afterwards on an ongoing basis. ASM allows you to monitor and manage any top-level shared folders created on your HP All-in-One Storage System using ASM or other applications, such as Windows Explorer or the Shared Folder MMC snap-in.

After shared folders are created, communication between client and host takes place over the Common Internet File System (CIFS) protocol.

Nested shared folders, which are shared folders that reside inside top-level shared folders, cannot be created using ASM, but can be viewed in ASM by selecting the top-level shared folder in the content pane and then clicking **Properties** in the Action pane. Use other applications, such as Windows Explorer or the Shared Folder MMC snap-in, to create nested shared folders on your HP All-in-One Storage System.

About the user interface



1 Menu bar

2 Toolbar

3 Navigation pane

4 Content pane

5 Actions pane

6 Status bar

Figure 16 ASM main window

Menu bar

The menu bar, located at the top of the ASM main window, is the Microsoft Management Console (MMC) menu bar. See the MMC online help for more information. To open MMC online help, click **Help** in the Actions pane.

Toolbar

The toolbar, located just below the menu bar in the ASM main window, is the MMC toolbar. See the MMC online help for more information. To open MMC online help, click **Help** in the Actions pane.

Navigation pane

The Navigation pane, located on the left side of the ASM main window, allows you to quickly navigate between HP All-in-One Storage Management applications.

Content pane

The content pane, located in the center of the ASM main window, displays application storage and storage component (logical disk and volume) properties, such as allocated and used space, using an expandable and collapsible view based on hierarchy.

The information displayed in the content pane depends on the item selected in the Filters drop-down menu, located at the top of the content pane, and the view selected in the Actions

pane. See "Monitoring storage" on page 93 for more information on views and information displayed in the content pane.

Filters drop-down menu

Select an application from the Filters drop-down menu, located at the top of the content pane, to view information for only that application in the content pane. Select **All** from the Filters drop-down menu to view information for all applications and shared folders in the content pane.

Actions pane

The Actions pane, located on the right side of the ASM main window, provides a list of actions available to the item currently selected in the content pane. Along with other selectable items, the Actions pane provides access to storage-allocation wizards that walk you through the process of hosting application storage and creating shared folders.

Table 16 Actions pane quick reference

Menu	Description
Application View	Displays the used and allocated storage space, and storage status of Exchange storage groups, SQL Server databases, user-defined storage, and shared folders hosted on your HP All-in-One Storage System in the content pane. See "Application View" on page 93 for more information.
Storage View	Displays the used and allocated storage space of the storage areas (logical disks and volumes) on your HP All-in-One Storage System that were created by ASM to store application data and shared folders in the content pane. See "Storage View" on page 105 for more information.
Application Server View	Displays your HP All-in-One Storage System and the application servers with storage hosted on your HP All-in-One Storage System in the content pane. See "Application Server View" on page 108 for more information.
Storage Utilization View	Displays the allocated storage values for specific applications and the shared folders pool, the unallocated storage value, and the storage value for data not managed by ASM in a pie chart. See "Storage Utilization View" on page 110 for more information.
Tools > Task Viewer	Opens the Task Viewer, where you can view the: • Status of tasks completed or scheduled to run in the future. • All tasks that failed and the errors reported. The Task Viewer also allows you to cancel running and scheduled tasks. See "Monitoring task completion status" on page 79 for further information.
Tools > Display Options	Displays the Configure Options window, where you can: • Change the colors used in the content pane to display the different types of storage, volumes, and servers. • Change the scaling used in the content pane so the size at which each application area or shared folder is displayed is proportional to the size of its allocated storage space, or to display them all at equal size. See "Defining user interface options" on page 58 for further information.
Refresh	Refreshes the content pane.

Menu	Description
Any one of the following items: • Host an Exchange Storage Group • Create a Shared Folder • Host a SQL Server Database • Host a User-Defined Application	Opens a storage-allocation wizard that helps you allocate and configure storage space on your HP All-in-One Storage System.
View > Customize	This is an MMC command. See the Microsoft Management Console online help. To open MMC online help, click **Help** in the Actions pane.
Help	Opens online help for ASM.
Allocate Space	Opens the Allocate Space Wizard where you can change the following storage configurations for the item selected in the content pane: • Size of allocated storage • Percentage full warning threshold • Enforced allocated limit (shared folders only) See Table 19 on page 72 for more information.*
Remove from View	Removes the application component or user-defined application selected in the content pane from view. Application areas removed from view can no longer be managed or monitored using ASM, but the application storage remains hosted on your HP All-in-One Storage System.See "Removing application areas from view" on page 91 for more information.*
Properties	Opens the Properties window where you can view the properties for the item selected in the content pane. See "Accessing application and shared folder properties" on page 94, "Accessing storage area properties" on page 106, and "Accessing application server properties" on page 108 for more information.*
Data Protection	Opens the Data Protection tab of the Properties window where you can schedule backups, run a backup, or restore data from a backup. You can also schedule snapshots, take a snapshot, expose a snapshot, or revert data to a past snapshot. See "Data protection" on page 81 for more information.*
* These actions can also be selected by right-clicking an item in the content pane.	

Defining user interface options

ASM allows you to customize the user interface color and scale settings.

Changing color settings

Changing color settings customizes the color used in the content pane to display the different types of storage, volumes, and servers. Colors help distinguish the different types of storage, storage areas, and servers from each other.

1. In the Actions pane, select **Tools > Options**.

   The Configure Options window opens.

2. Click the **Colors** tab.

3. Select an item in the Items list and a color in the Color drop-down menu.
4. When your color selections are complete, click **Apply** to apply the color settings to the content pane.
5. Click **OK**.

Scaling display settings

Changing the scaling settings customizes the size at which each application area or shared folder is displayed in the content pane. You can choose to scale each application area and shared folder so that it is displayed in proportion to its capacity (allocated storage size), or so that all the application areas and shared folders are displayed at the same size.

1. In the Actions pane, select **Tools > Options**.

   The Configure Options window opens.
2. Click the **Scaling** tab.
3. Select the storage-display proportion setting:
   - According to capacity, using automatic scaling—Displays logical disks and volumes, and application areas according to relative size, but leaves the display readable.
   - All as the same size—Displays logical disks and volumes, and application areas as the same size.
4. Click **Apply** to apply your change.
5. Click **OK**.

Add an All-in-One Storage System

You may add another All-in-One Storage System for the ease of managing more than one All-in-One from the same console. To add another All-in-One Storage System:

1. Click on **Add All-in-One Storage System** in the Actions pane.
2. A dialog box will open. Enter the hostname or IP address of the All-in-One Storage System to add.
3. The added All-in-One Storage System will appear in the Navigation pane.

Remove an All-in-One Storage System

To remove an added All-in-One Storage System:

1. Click on **Remove All-in-One Storage System**.
2. A window will appear, asking if you would like to remove the All-in-One Storage System
3. Click **Yes**.

4 Hosting storage for applications and shared folders

The All-in-One Storage Manager (ASM) radically simplifies hosting application storage and shared folders on your HP All-in-One Storage System, using storage-allocation wizards. Use storage-allocation wizards to allocate and configure storage for these applications:

Application	Description	Notes
Exchange	Allocate and configure storage for one or more Exchange storage group components. A wizard assists you by discovering Exchange storage group components (such as mail stores, public stores, and logs), suggesting default storage configurations based on best practices for Exchange, migrating the Exchange storage group components you selected to your HP All-in-One Storage System, and configuring Exchange to store data on your HP All-in-One Storage System.	See "Using the Host an Exchange Storage Group Wizard" on page 62 .
Shared Folders	Create shared folders on your HP All-in-One Storage System. A wizard assists you in allocating and configuring storage space for shared folders, and creating shared folders.	See "Using the Create a Shared Folder Wizard" on page 64 .
SQL Server	Allocate and configure storage for SQL Server databases. A wizard assists you by discovering servers that host SQL Server and SQL Server database components (such as data files and logs), suggesting default storage configurations based on best practices for SQL Server, migrating the SQL Server database components you selected to your HP All-in-One Storage System, optionally deleting the SQL Server database components you selected from the server that hosts SQL Server, and configuring SQL Server to store data on your HP All-in-One Storage System.	See "Using the Host a SQL Server Database Wizard" on page 65.
User-Defined Applications	Allocate and configure storage for any remote application over the iSCSI protocol or any other application that requires storage on the All-in-One Storage	See "Using the Host a User-Defined Application Wizard" on page 67.

Application	Description	Notes
	System. A wizard assists you in allocating and configuring storage space. The wizard does not migrate user-defined application data to your HP All-in-One Storage System or reconfigure the application to store data on your HP All-in-One Storage System. You must do this manually as described in "Migrating user-defined application data from a remote application" on page 80, and as described in the application's documentation.	
Data Protection	Create a virtual library that backs up data from a remote system on your All-in-One Storage System. A wizard assists you in choosing size and storage allocation.	See "Using the Create a Virtual Library Wizard" on page 68.

Using the Host an Exchange Storage Group Wizard

The **Host an Exchange Storage Group Wizard** automatically discovers the Exchange storage groups in your network domain and helps you allocate and configure storage space for these components:

- Mail stores—Contain the data in user mailboxes.
- Public stores—Contain the data in public folders.
- Logs—Provide a record of every message stored in a storage group.

Before you begin configuring storage for Exchange

- Make sure the ASM agent is installed on each server with Exchange data you plan to host. See Installing the All-in-One Storage Manager Agent on network application servers for more information.
- Make sure you have a current backup of your Exchange data and logs.

Accessing the Host an Exchange Storage Group Wizard

1. In the Actions pane, select **Host an Exchange Storage Group**.

   The**Host an Exchange Storage Group Wizard** welcome page opens.

2. Click **Next** to open the Specify Exchange Server page (see "Entering a name of a server that hosts Exchange" on page 62).

Entering a name of a server that hosts Exchange

Use the Specify Exchange Server page to provide ASM with the name or the Internet Protocol (IP) address of a remote server in your current domain that hosts Exchange.

1. Do one of the following:
   - Enter the host name of a server that hosts Exchange (exactly as it is registered in the domain).
   - Enter the IP address of a server that hosts Exchange.

2. Click **Next** to open the Select Storage Group Components page (see "Selecting Exchange Server storage group components" on page 63).

Selecting Exchange storage group components

Use the Select Storage Group Components page to select the Exchange storage group and storage group components (mail stores, public stores, and logs) you want to host on your HP All-in-One Storage System and manage using ASM.

1. Do one of the following:
   - Select the entire storage group (including all of its components) by checking the box next to the storage group.
   - Select individual storage group components by expanding the list and checking the boxes next to the components.

   You must select all the storage group components in a storage group if you want to run backups or take snapshots of the Exchange storage group using ASM.

   The table below lists the action ASM will perform for each storage group component selected.

   Table 17 Selecting storage group components to host

Action	Description
None	Component's check box is not selected, so ASM will not perform any action. Select check box to change action.
Allocate Space, Move Data	Storage space will be allocated and configured on your HP All-in-One Storage System. Component's data will be migrated to your HP All-in-One Storage System.
None, Already Managed	Component's data is already hosted on your HP All-in-One Storage System and already managed by ASM. No action is possible.

2. To view the properties for a storage group component, select the storage group component name and then click **Properties**.

   See "MailStore database properties" on page 96, "PublicStore database properties" on page 97, and "Log properties for storage group" on page 97 for descriptions of the properties displayed.

3. When you are done, click **Next** to open the Storage Allocation page (see "Allocating space for components" on page 69).

Local Continuous Replication (LCR)

If the Local Continuous Replication (LCR) feature is enabled in Microsoft Exchange 2007, you have the option of migrating LCR components to your All-in-One Storage System. LCR components are shown in the Select Storage Group Components page in the wizard if this feature is enabled. They are selected in the same manner as other Exchange components.

NOTE:

It is not recommended to host both the LCR and the original Exchange components on a single All-in-One Storage System.

Using the Create a Shared Folder Wizard

The **Create a Shared Folder Wizard** walks you through the process of creating a top-level shared folder (file share) on your HP All-in-One Storage System, including allocating and configuring the required storage.

NOTE:

You cannot create nested shared folders on your HP All-in-One Storage System using ASM. You may use other applications, such as Windows Explorer or the Shared Folder MMC snap-in, to create nested shared folders on your HP All-in-One Storage System.

You can view the nested shares in a top-level shared folder by selecting the top-level shared folder in the content pane, clicking **Properties** in the Action pane, and then clicking the **Nested Shares** tab.

Accessing the Create a Shared Folder Wizard

1. In the Actions pane, select **Create a Shared Folder**.

   The Create a Shared Folder Wizard welcome page opens.

2. Click **Next** to open the **Enter a Shared Folder Name and Description** page (see "Naming a shared folder" on page 64).

Naming a shared folder

Use the **Enter a Shared Folder Name and Description** page to provide ASM with a name and description for the shared folder.

1. Enter the name for the shared folder.

   NOTE:

   The path to the shared folder is created by ASM and is based on the shared folder name. The Share Path field is *Read Only*.

2. Enter a description of the shared folder (optional).
3. Click **Next** to open the Set Shared Folder Permissions page (see "Setting permissions for a shared folder" on page 64).

Setting permissions for a shared folder

Use the Set Shared Folder Permissions page to set network user read and write permissions for the shared folder.

NOTE:

Permissions can be further customized using Windows administration tools, such as Windows Explorer and the Shared Folder MMC snap-in.

1. Select a permission level.

2. Click **Next** to open the Storage Allocation page (see "Allocating space for components" on page 69).

Using the Host a SQL Server Database Wizard

The Host a SQL Server Database Wizard automatically discovers the servers that host SQL Server and SQL Server databases on your domain, and helps you allocate and configure storage space for each database component you select:

- Data file—Contains pointers to database files, storage for system tables and objects, and storage for database data and objects.
- Log file—Holds all the transaction log information for the database. Every database has exactly one log file, which cannot be used to hold any other data.

Before you begin configuring storage for SQL Server

- Make sure the ASM agent is installed on each server with SQL Server data you plan to host. See "Installing the All-in-One Storage Manager Agent on network application servers" on page 33 for more information.
- Make sure you have a current backup of your SQL Server data and logs.

Accessing the Host a SQL Server Database Wizard

1. In the Actions pane, select **Host a SQL Server Database**.

   The Host a SQL Server Database Wizard welcome page opens.
2. Click **Next** to open the **Select a SQL Server** page (see "Selecting a server that hosts SQL Server" on page 65).

Selecting a server that hosts SQL Server

Use the Select a SQL Server page to select one of the servers that hosts SQL Server discovered on your domain by the wizard.

1. Do one of the following:
   - Enter the host name of a server that hosts SQL (exactly as it is registered in the domain).
   - Enter the IP address of a server that hosts SQL.
2. Click **Next** to open the **Select Database Components** page (see "Selecting SQL Server database components" on page 65).

Selecting SQL Server database components

Use the **Select Database Components** page to select the SQL Server database and database components you want to host on your HP All-in-One Storage System.

1. Do one of the following:
   - Select all components (including all of its components) by checking the box next to the component.
   - Select individual database components by expanding the list and checking the boxes next to the components.

   You must select all the database components, including the log file, in a database if you want to run backups and/or take snapshots of the database using ASM.

NOTE:

ASM cannot migrate system databases; for example, ASM cannot migrate `master`, `model`, `msdb` and `tempdb`.

The following table lists the action ASM can perform for each database component listed.

Table 18 Selecting database components to host

Action	Description
None	Component's check box is not selected, so ASM will not perform any action. Select check box to change action.
Allocate Space, Move Data	Storage space will be allocated and configured on your HP All-in-One Storage System. Component's data will be migrated to your HP All-in-One Storage System.
None, Already Managed	Component's data is already hosted on your HP All-in-One Storage System and already managed by ASM. No action is possible.

2. To view the properties for a database component, select the database component name and then click **Properties**.

   See "Data file properties" on page 101 and "Log file properties for database" on page 101 for descriptions of the properties displayed.
3. If you do not want ASM to delete the original files for the selected database components from the server that hosts SQL Server after it migrates the data to your HP All-in-One Storage System, clear the **Delete original files after successful migration** checkbox.
4. When you are done, click **Next** to open the **Select the Database Workload Type** page (see "Selecting a database workload type" on page 66).

Selecting a database workload type

Use the Select the Database Workload Type page to select the workload type for the SQL Server database.

NOTE:

You can only select the database workload type while using the Host a SQL Server Database Wizard. The database workload type cannot be changed later.

1. Do one of the following:
   - Select **Transaction processing (TP)** for frequently updated, fast growing databases with large volumes of data requiring concurrent user access.
   - Select **Decision support systems (DSS)** for databases designed to handle queries on large amounts of data, typically used for data-mining applications.
2. When you are done, click **Next** to open the **Storage Allocation** page (see "Allocating space for components" on page 69).

Using the Host a User-Defined Application Wizard

This wizard helps you set up your All-in-One Storage System to store application data for various applications. Storage is allocated for the application, optionally exposed to another server using the iSCSI protocol, and an NTFS file volume may be optionally created on the remote application server. Upon completion, you can monitor and manage storage for the application through the All-in-One Storage Manager.

After storage is allocated and configured on your HP All-in-One Storage System for a remote application using the Host a User-Defined Application Wizard, do the following:

- Manually migrate the remote application's data to your HP All-in-One Storage System. See "Migrating user-defined application data from a remote application" on page 80 for more information.
- Configure the remote application to store its data on the iSCSI LUN exported by ASM to the application server as described in the application's documentation.

Before you begin configuring storage for a user-defined application

- Make sure the ASM agent is installed on each application server with data you plan to host.
- Make sure you have a current backup of your remote application data and logs.
- For Remote Windows Applications:
  - Runs under Windows Server 2003
  - Uses NTFS volumes for storage
- For an iSCSI LUN application, you will need the iSCSI qualified name.

NOTE:

For a remote Windows application, you need to know the path to the iSCSI LUN on the application server to configure the remote application to store data on the iSCSI LUN. The path to the iSCSI LUN is displayed on the application's Properties window on the Storage tab.

To access the Host a User-Defined Application Wizard

1. In the Actions pane, select **Host a User-Defined Application**.

   The Host a User-Defined Application Wizard welcome page opens.
2. Click **Next** to open the Choose type of Application page (see "Choose type of application" on page 68).

Choose type of application

1. Select the type of application for hosting a user-defined application:
   - Remote Windows Application- ASM will provision storage for the application and expose the storage to the given server as an NTFS volume over the iSCSI protocol. This is the recommended option for most scenarios. The All-in-One Storage Manager agent must be installed on the application server to use this option.
   - iSCSI LUN- Exposes a LUN to the remote server so the server can store data on the LUN. You will need to install an iSCSI initiator on your host server. Storage is provisioned for these applications.
   - Local storage only- Creates a volume on your All-in-One Storage System. Storage is provisioned for these applications.
2. Click **Next** to open the Enter an Application Name page (see "Entering an application name" on page 68).

Entering an application name

Use the Enter an Application Name page to enter a name for the application. This name will be used anywhere the application is referenced in ASM, so it must be a *unique* name.

1. Enter a name for the application.
2. When you are done, click **Next** to open the Storage Allocation page (see "Allocating space for components" on page 69).

Using the Create a Virtual Library Wizard

This wizard helps you create a virtual library for disk-to-disk backup of other client or servers to your All-in-One Storage System and manage the storage for the virtual library through ASM. Install Data Protector Express on additional servers you need to backup. See

Accessing the Virtual Library Wizard

To access the Create a Virtual Library Wizard

1. In the Actions pane, select **Create a Virtual Library**.

   The Create a Virtual Library welcome page opens.
2. Click **Next** to open the Configure virtual library page (see "Configure your virtual library" on page 68).

Configure your virtual library

To configure your virtual library, do the following:

1. In the name dialog box, type a name for your virtual library.
2. In the **Number of slots** field, type or use the arrows to indicate how many slots are needed for your virtual library.

3. When you are done, click **Next** to open the Storage Allocation page (see "Allocating space for components" on page 69).

NOTE:

The number of slots needed for your virtual library will depend on the media rotation type chosen for the backups that will use the virtual library. The number of slots must be high enough to support the rotation type you intend to use for scheduling backups to this virtual library. See *Planning for Media Rotation* in the *Data Protector Express User's Guide and Technical Reference* for more information.

Allocating space for components

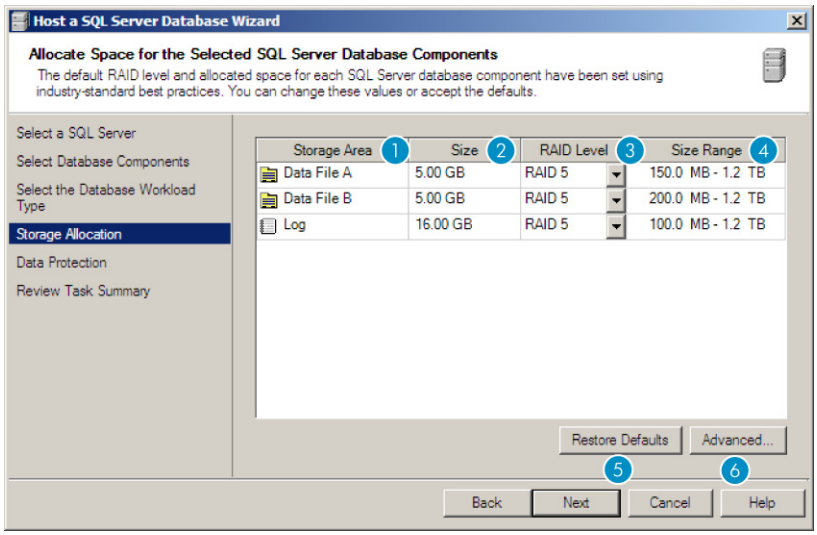
Use the **Storage Allocation** page in the wizards to specify the allocated space size and advanced configuration settings for each application component or shared folder listed. Default values are provided.

NOTE:

15 MB is the minimum value that can be allocated. You cannot set the size below the minimum value.

NOTE:

SQL Server and Exchange default advanced configuration settings are based on SQL Server, Exchange, and HP storage best practices, and should generally not be changed.



1. Application components, user-defined application, or shared folder name

2. Specify size of storage space to allocate to each application component, user-defined application, or shared folder listed

3. Specify the storage RAID level for each application component, user-defined application, or shared folder listed

4. Minimum and maximum storage space that can be allocated to each application component, user-defined application, or shared folder listed

5. Reset all values to defaults

6. View/change advanced configuration settings for each application component, user-defined application, or shared folder listed

Figure 17 Storage Allocation page

1. Do one of the following:
   - Click **Next** to accept the default values that ASM has provided for the components, user-defined application, or shared folder selected.
   - Change the default size values:
     - Select a row to edit.
     - Highlight the storage size unit value and then enter a new value as necessary: megabytes (MB), gigabytes (GB), or terabytes (TB).
     - Highlight the storage size number value and enter a new value, or click the arrow buttons to change the value.

NOTE:

The **Size Range** column shows the minimum and maximum storage space that can be allocated to each application component, user-defined application, or shared folder listed. Whenever you change the allocated space size or an advanced configuration setting for an application component, the maximum value for **Size Range** is recalculated for all the application components listed.

NOTE:

To change the advanced configuration settings for an application component, user-defined application, or shared folder listed, select the item to edit and then click **Advanced**. See "Selecting advanced configuration settings" on page 71 for more information.

2. When you are done selecting the storage allocation and configuration settings, click **Next** to open the summary page.

NOTE:

After storage space is allocated and configured using a wizard, only the following storage configuration settings can be changed:

- Allocated space size
- Percent full warning threshold
- Enforce Allocated Limit (shared folders and local storage applications)

After a logical disk is created, its configuration cannot be changed.

Selecting advanced configuration settings

Use the **Advanced** window in the wizard to change the allocated space size and default advanced configuration settings for each application component, user-defined application, and shared folder listed.

After storage is configured using a wizard, you can access the Advanced window from the Allocate Space Wizard and change the allocated space size, percent full threshold warning, and/or enforce allocated limit (shared folders and local storage applications) values as needed.

Table 19 provides a brief description of the items you can modify:

Table 19 Advanced window items

Item	Description	Notes
Size	The amount of storage that ASM allocates to the application component, user-defined application, or shared folder you are configuring.	You are prevented from setting the size below 15 MB. After the allocated storage space is full (100 percent used), no further data can be stored to the space until you increase the size using the Allocate Space Wizard. The only exception is for shared folders and local storage applications without an enforced allocated limit. If there is unused storage space on the logical disk where a component without an enforced allocated limit resides, data can be written to the component until the logical disk is full.
RAID Level	Hard drive formatting that provides different levels of performance, capacity, and data protection.	For more information about RAID levels, see Customizing RAID levels on page 73.*
RAID Stripe Size	The number of bytes or kilobytes of data in each RAID stripe (block of data). The RAID stripe size selected affects performance. For the best performance, select the stripe size closest to the size of the files being saved.	ASM provides the following general values: small (8 kB), medium (16 kB), and large (64 kB).*
Percent Full Warning Threshold	The percent full value that when reached changes the storage status to Warning and issues a warning alert. The warning indicates that storage use has surpassed the percentage full value. For example, if you enter 75%, you see a warning (yellow asterisk) in the content pane when storage is at 75 percent full.	The percent full warning threshold is set by default to 80%. Percent full warning threshold values are ASM-specific; percent full warning threshold values selected in the Quota Management MMC snap-in are not adopted by ASM. All other Quota Management MMC snap-in settings are adopted by ASM. See Setting a percent full warning threshold on page 74.
Exclusive Storage	Data is stored on hard drives dedicated to storing only the data for the application component, user-defined application, or shared folder you are configuring. The number of hard drives dedicated depends on the allocated space size and other advanced storage configuration settings selected for the item you are configuring. Exclusive storage is recommended for some applications for the storage of specific types of data.	For Exchange and SQL Server, ASM default values specify exclusive storage for log files, which according to storage best practices, should be isolated from other application storage areas.*
Enforce Allocated Limit (Quota)	Sets an enforced quota for the amount of storage available to a shared folder or local storage	This item is available for shared folders and local storage component. See Enforcing an

Item	Description	Notes
	application. When the storage space allocated to a component is full, no further data can be saved to this component.	allocated storage limit for shared folders and local storage applications on page 75.
Hot Spare Required	A hot spare is a hard drive reserved as a spare for storage space configured as RAID 1, 1+0, 5, or 6. A hot spare automatically replaces a hard drive when it fails. When the failed hard drive is replaced, its replacement becomes the new hot spare.	A hot spare is assigned at the array level. A LUN that does not require a hot spare may be assigned one anyway if another LUN on the same array requires a hot spare. *
Physical Disk Type	Type of physical disk to add for the hot spare	You are able to choose SAS, (Serial Attached SCSI) SATA, (Serial Advanced Technology Attachment) or SCSI (Small Computer System Interface) for a physical disk type.*
*After you have allocated and configured storage for an application component, user-defined application, or shared folder using a wizard, you can change the allocated space size, change the percent full warning threshold, and change the enforced allocated limit (shared folders and local storage applications). However, you cannot change the RAID level, RAID stripe size, Hot Spares, Physical Disk Type, or Exclusive Storage settings.		

Customizing RAID levels

Before you customize the default RAID level setting, review Table 20 to see how the different RAID levels affect performance, capacity, and data protection level.

Unless you customize the advanced configuration settings, the wizard configures the storage space with the default values shown on the Advanced window:

- For Exchange and SQL Server, the wizard suggests default settings based on HP storage best practices and specific recommendations for Exchange storage group and SQL Server database components. You should generally accept these defaults.
- For user-defined applications and shared folders (where industry-standard recommendations cannot be determined), the wizard provides default settings you can customize.

Table 20 shows how the different RAID levels affect:

- Performance–The speed at which data is read from and written to the hard drives. The RAID level with the best performance rating provides the fastest reads and writes.
- Capacity–The available storage space on the hard drives. The RAID levels with the best capacity rating require the least amount of storage space to store data.
- Data protection–The number of hard drives that can fail without data being lost. The RAID level with the best data protection rating allows more hard drives to fail before data is lost.

For more information on the different RAID levels, see Table 20.

Table 20 Descriptions of RAID levels

RAID level	Description
No RAID	Offers no protection against disk failure. If a disk drive fails, data is lost.
RAID 0 – Striping (No Fault Tolerance)	Offers the greatest capacity and performance without data protection. If you select this option, you will experience data loss if a hard drive

RAID level	Description
	that holds the data fails. However, because no logical drive capacity is used for redundant data, this method offers the best capacity. This method offers the best processing speed by reading two stripes on different hard drives at the same time and by not having a parity drive.
RAID 1 – Mirroring	Offers a good combination of data protection and performance. RAID 1 or drive mirroring creates fault tolerance by storing duplicate sets of data on a minimum of two hard drives. There must be an even number of drives for RAID 1. RAID 1 and RAID 1+0(10) are the most costly fault tolerance methods because they require 50 percent of the drive capacity to store the redundant data. RAID 1 mirrors the contents of one hard drive in the array onto another. If either hard drive fails, the other hard drive provides a backup copy of the files and normal system operations are not interrupted.
RAID 1+0 – Mirroring and Striping	Offers the best combination of data protection and performance. RAID 1+0 or drive mirroring creates fault tolerance by storing duplicate sets of data on a minimum of four hard drives. There must be an even number of drives for RAID 1+0. RAID 1+0(10) and RAID 1 are the most costly fault tolerance methods because they require 50 percent of the drive capacity to store the redundant data. RAID 1+0(10) first mirrors each drive in the array to another, and then stripes the data across the mirrored pair. If a physical drive fails, the mirror drive provides a backup copy of the files and normal system operations are not interrupted. RAID 1+0(10) can withstand multiple simultaneous drive failures, as long as the failed drives are not mirrored to each other.
RAID 5 – Distributed Data Guarding	Offers the best combination of data protection and usable capacity while also improving performance over RAID 6. RAID 5 stores parity data across all the physical drives in the array and allows more simultaneous read operations and higher performance than data guarding. If a drive fails, the controller uses the parity data and the data on the remaining drives to reconstruct data from the failed drive. The system continues operating with a slightly reduced performance until you replace the failed drive. RAID 5 can only withstand the loss of one drive without total array failure. It requires an array with a minimum of three physical drives. Usable capacity is N-1 where N is the number of physical drives in the logical array.
RAID 6– Advanced Data Guarding (ADG)	Offers the best data protection and is an extension of RAID 5. RAID 6 uses multiple parity sets to store data and can therefore tolerate up to 2 drive failures simultaneously. RAID 6 requires a minimum of 4 drives and is available only if the controller has an enabler. Writer performance is lower than RAID 5 due to parity data updating on multiple drives. It uses two disk for parity; its fault tolerance allows two disks to fail simultaneously. Usable capacity is N-2 where N is the number of physical drives in the logical array.

Setting a percent full warning threshold

To receive a warning alert when storage capacity reaches a specified limit, set the *percent full warning threshold*. You can set a warning threshold for any application component, user-defined application, and shared folder that ASM manages. An iSCSI LUN application will not have a warning threshold.

By default, the warning threshold is set to 80%. To change it, enter a new percent value on the Advanced window.

After you set a warning threshold, ASM changes the status indicator for the application component, user-defined application, or shared folder when this threshold has been surpassed. This is a warning only; no hard limits are enforced on storage capacity as a result of setting this value. The warning is visible in these places:

- A yellow warning icon appears on the application component, user-defined application, or shared folder icon in the content pane.
- As an *alert* in the Properties window.

NOTE:

For shared folders and local storage applications, you can set an enforceable limit (or quota) for allocated storage, as well as a warning threshold. For more information, see
Enforcing an allocated storage limit for shared folders and local storage applications.

Enforcing an allocated storage limit for shared folders and local storage applications

ASM provides a way to enforce an allocated storage limit for shared folders and local storage applications. If enforced, the system does not allow the amount of allocated space for a shared folder and local storage application to be exceeded.

If the capacity of the shared folder and/or local storage application surpasses the percent full warning threshold and reaches the allocated space limit, the status changes from *Warning* to *Critical* in the content pane, and users are blocked from adding data to the shared folder and local storage application.

NOTE:

If you do not choose to enforce an allocated storage limit for a shared folder, the ASM status indicator still goes from *Warning* to *Critical* in the content pane; however, users are not blocked from adding data to the shared folder as long as there is still unallocated storage space on the logical disk where the shared folder resides. Data can be written to the shared folder until the logical disk is full.

By default, the Enforce Allocated Limit (Quota) is set to **No** for all shared folders and local storage applications. To change this setting, do one of the following:

- Using the Create a Shared Folder Wizard, change the Enforce Allocated Limit (Quota) setting on the Advanced window to Yes.
- Select the shared folder in the content pane, click **Properties** in the Actions pane, click the **Warning Threshold** tab, and then select the **Enforce Allocated Limit (Quota)**.
- Select the shared folder in the content pane, click **Allocate Space** in the Actions pane, click **Advanced**, and then change the Enforce Allocated Limit (Quota) setting to **Yes**.

NOTE:

If a Shared Folder is created outside of ASM, you must run the Allocate Space Wizard on the particular folder to enable the Enforce Allocated Limit (Quota) setting.

To allocate space for a shared folder, specify a size using the Allocate Space Wizard as described in "Increasing or reducing the allocated storage" on page 89.

Selecting data protection

Use the Data Protection window in the wizard to select the following:

- Local disk backup- Previous versions of data are retained on disk using virtual library backups and/or volume snapshots for fast recovery.
- Alternate location backup— Data is copied off of this All-in-One Storage System to tape, other disks, or other types of storage media. This enables long term storage and disaster recovery.
- Modify Advanced Properties:
  - Scheduling backups, page 77, of an Exchange storage group, SQL Server database, user-defined application, or shared folder for local disk backup or an Alternative location backup.
  - Scheduling snapshots, page 78, of an Exchange storage group, SQL Server database, user-defined application, or all the shared folders on the same volume for a local disk backup or an Alternative location backup.

NOTE:

Backups and snapshots are disabled for an Exchange storage group or a SQL Server database if not all the components of the Exchange storage group or SQL Server database are selected on the **Select components to host** page of the wizard.

NOTE:

Snapshots are taken at the volume level. See "Storage View" on page 105, for information on viewing volumes.

After you have selected data protection settings, click **OK**.

Before you schedule backups

Before you schedule backups:

- Before you schedule alternate location backups, install a tape library or other physical device and add it to the same Data Protector Express Management Domain as your HP All-in-One Storage System.
- Installing a tape library that can accommodate the media rotation type required by your environment requires tape storage management experience. See http://www.hp.com/sbso/serverstorage/ultimate.html to learn more about tape storage.

Scheduling backups

1. On the Data Protection page in any wizard, select **Modify Advanced Properties**. This will open the **Data Protection Advanced Properties** window.

> NOTE:
>
> You are also able to get to the Data Protection Advanced Properties window by selecting the Data Protection action on the selected component after you have completed the wizard. See Selecting local or alternate backup for more information on how to navigate to the Data Protection page outside of a wizard.

2. In the Data Protection Advanced Properties window, select **Schedule backups to a virtual library** to enable the backup schedule or leave unselected to suspend backups for now.
3. Select either **Local Disk Backup** or **Alternate Location Backup**
4. Select a Data Protector Express media rotation type from the list.
5. Type or use the arrows to indicate a time for the backup to begin.
6. For **Local Disk Backup**, select the size for the virtual library. A default value will be recommended, based on the selected rotation type and component size. Click on *Modify Advanced Properties* to modify advanced storage settings such as RAID level and stripe size. See Selecting advanced configuration settings for more information on advanced properties.
7. For **Alternate Location Backup**, select the device for the virtual library to reside.

Although it is not required, after you finish creating a backup job using a wizard or a components property page, you can modify the backup job properties in Data Protector Express. For example, you may want to enable encryption or customize a media rotation type.

1. Launch Data Protector Express.
2. On the login window:
   a. Enter `localhost` in the **Host name** field.
   b. Enter `ASMbackup` in the **User name** field.

> △ CAUTION:
>
> The default password for ASMbackup is blank. It can be changed in the Command Line Interface (CLI).

   c. Click **OK**.
3. Click **Jobs and Media** in the Favorites pane, located on the left side of the main window.
4. Double-click **ASMbackup** on the right side of the main window.
5. Select the backup job for the application or shared folder whose backup schedule you want to edit.
6. Right-click the file and select **Properties**.

See the *HP StorageWorks Data Protector Express Users Guide and Technical Reference* for more information.

Scheduling snapshots

1. On the Data Protection page in any wizard, select **Modify Advanced Properties**. This will open the **Data Protection Advanced Properties** window.

NOTE:

You are also able to get to the Data Protection Advanced Properties window by selecting Data Protection after you have scheduled backups. See Selecting local or alternate backup for more information on how to navigate to the Data Protection page outside of a wizard.

2. Click the box on the right side of the Snapshot Schedules box to open the Snapshot Schedule page.
3. Click **Add** to add a snapshot to the snapshot schedule.
4. Select a snapshot frequency (hourly, daily, weekly, monthly) for snapshots.
5. Enter a start date for snapshots.
6. Enter a start time for snapshots.
7. To add another snapshot to the snapshot schedule, repeat steps 2 through 5.
8. To delete a snapshot from the snapshot schedule, select the snapshot and click **Remove**.
9. Click **OK** to save your changes and return to the Data Protection page.

The Schedules box now displays the snapshots added, or displays **Aggregate Schedule** if more than one snapshot was added to the snapshot schedule.

Reviewing task summary and scheduling tasks

1. Review the list of tasks the wizard will perform to allocate and configure storage, and to host the application storage or shared folder on your HP All-in-One Storage System.

   For application storage, ensure the following is true before you run the tasks:

   - You have an up-to-date backup of the application data and logs.
   - The application data and logs are not being accessed or modified.
2. Do one of the following:

   - To go back and change your selections, click **Back**.
   - To run the listed tasks immediately, click **Finish**.
     - The Task Viewer opens, running the tasks required to configure storage and migrate data. See Monitoring task completion status for more information.
   - To schedule tasks to run at a later time, select **Schedule tasks to run later**, enter a start date and time, and then click **Finish**.

     To select AM or PM for the start time, click the up and down arrow buttons.

     To use a calendar to select a start date, click the down arrow button (located to the right of the up and down arrow buttons) to open a calendar. To change the month displayed on the calendar, click the previous and next buttons on the calendar, or click on the month or year displayed at the top of the calendar to display drop-down lists.

Monitoring task completion status

The Task Viewer shows the status of ASM wizard tasks. ASM wizard tasks allocate and configure storage, host application storage and shared folders, and configure data protection.

NOTE:

Click the Expand tree icon next to a task to view its subtasks.

Select a task to view its description in the Details box on the Task Viewer.

The Task Viewer has a filter drop-down menu. Each selection displays information about task-completion status for different time periods:

- Show All—Displays all tasks that have been completed or failed to complete. Displays the tasks and subtasks currently being processed and all scheduled tasks.
- Today—Displays the tasks and subtasks currently being processed, all scheduled tasks, and tasks that completed or failed today.
- Last 3 Days—Displays the tasks and subtasks currently being processed, all scheduled tasks, and tasks that completed or failed during the past three days, including today.
- Last 7 Days—Displays the tasks and subtasks currently being processed, all scheduled tasks, and tasks that completed or failed during the past seven days, including today.
- Last 30 Days—Displays the tasks and subtasks currently being processed, all scheduled tasks, and tasks that completed or failed during the past thirty days, including today.
- Errors Only—Displays all tasks that have failed and provides information about problems that occurred during task processing.

The status of each task is provided and can be any one of the following:

- Scheduled—The task has been scheduled to run at a specified time.
- Verifying—ASM is confirming the configuration you specified is valid.
- Ready—The task is ready to run and is waiting for other tasks or background processes to run.
- Running—The task is being processed.
- Completed (date)—The task completed without problems.
- Cancelling—The task is being cancelled.
- Cancelled—The task has been cancelled (see Cancelling tasks).
- Failed—An error occurred during processing.

Cancelling tasks

1. To cancel an uncompleted task, select the task and click **Cancel Selected Task**.
2. Click **Yes** to confirm.

Tasks canceled after they have started may not cancel immediately. A task will stop running when the last subtask started is completed. All subtasks listed below the last completed subtask are not completed and cannot be restarted.

Migrating user-defined application data from a remote application

The Host an Exchange Storage Group Wizard and Host a SQL Server Database Wizard automatically migrate application data from the application server to your HP All-in-One Storage System. The Host a User-Defined Application Wizard, however, does not migrate data for a user-defined application from the application server to your HP All-in-One Storage System. You must do this manually.

1. Using ASM, determine the path to the iSCSI LUN (logical disk) created on the application server by ASM, as follows:
   a. Select the user-defined application in the content pane.
   b. In the Actions pane, select **Properties**.

      The Properties window opens.
   c. Click the **Storage** tab.
   d. Record the Application Path information displayed.
2. Copy the application data to the path on the application server recorded in step 1 as follows:
   a. Using Windows Explorer, navigate to the application data you want to host on your HP All-in-One Storage System.
   b. Copy the application data and paste it to the application path on the application server recorded in step 1.

      For example, if the application data is stored on `C:\application\data` and the application path you recorded is `G:\application\data`, copy and paste the data in `C:\application\data` to `G:\application\data` on the application server.
3. Delete the application data from the old path (optional).

Any data saved to the iSCSI LUN on the application server is now saved to a LUN on your HP All-in-One Storage System and not on the server.

5 Data protection

The Data protection window allows for the following:

- Select how data protection is configured, using local disk-to-disk (Local D2D) and/or Alternate Location Backup (D2Any) of an Exchange storage group, SQL Server database, user-defined application, or shared folder.
- Select a media rotation type for backups or run a backup of an Exchange storage group, SQL Server database, user-defined application, or shared folder. See "Scheduling and running backups" on page 84.
- Create a snapshot schedule, take a snapshot, or delete a snapshot of an Exchange storage group, SQL Server database, user-defined application, or shared folder. See "Scheduling snapshots" on page 82 and "Taking snapshots" on page 82.
- View the contents of a snapshot by exposing it. See "Exposing a snapshot" on page 83 and "Unexposing a snapshot" on page 83.
- Restore an Exchange storage group, SQL Server database, user-defined application, or shared folder from a backup. See "Restoring data from backups" on page 84.
- Revert an Exchange storage group, SQL Server database, or user-defined application to a past snapshot. See "Reverting data to snapshots" on page 83.

NOTE:

Backups and snapshots are disabled in ASM for an Exchange storage group or an SQL Server database if not all the components of the Exchange storage group or SQL Server database are hosted. To host components not yet hosted for a storage group or database, start the Host an Exchange Storage Group Wizard or Host a SQL Server Database Wizard as appropriate, select the storage group or database, and then select the components on the **Select components to host** page that are not yet hosted.

Data Protection Window

In the Data Properties window, you are able to select data protection features, modify advanced properties, and manage backups and snapshots.

Selecting local or alternate backup

You are able to select **Local Disk Backup** or **Alternate Location Backup**. Local Disk backup saves pervious version of data on disks, while Alternate Location Backup copies data to tape, other disks or other types of storage media.

1. Do one of the following:
   - Select an Exchange storage group in the content pane to schedule backups of the Exchange storage group.
   - Select a SQL Server database in the content pane to schedule backups of the SQL Server database.
   - Select a user-defined application in the content pane to schedule backups of the user-defined application.
   - Select a shared folder in the content pane to schedule backups of the shared folder.
2. Do one of the following:
   - In the Actions pane, click **Data Protection**.
   - In the Actions pane, click **Properties** and then select the **Data Protection** window.
3. You may select **Local Disk Backup** and/or **Alternate Location Backup** for any component.
4. Click on **Modify Advanced Properties** to set advanced properties of the backup and snapshot schedules. See Selecting data protection for more information on scheduling backups and snapshots.

Managing snapshots and backups

To manage snapshots and backups, first navigate to the Data Protection window:

1. Do one of the following:
   - Select an Exchange storage group (or a component of a storage group) in the content pane to schedule backups of the Exchange storage group.
   - Select an SQL Server database (or a component of a database) in the content pane to schedule backups of the SQL Server database.
   - Select a user-defined application in the content pane to schedule backups of the user-defined application.
   - Select a shared folder in the content pane to schedule backups of the shared folder.
2. Do one of the following:
   - In the Actions pane, click **Data Protection**.
   - In the Actions pane, click **Properties** and then select the **Data Protection** window.
3. Click on **Manage backups and snapshots**.

Snapshots

From the Manage backups and snapshots window, you are able to take snapshots, expose or unexpose them, and schedule them. See Managing snapshots and backups to navigate to the **Manage backups and snapshots** tab.

Scheduling snapshots

To schedule snapshots, see Scheduling snapshots on page 78 for more information.

Taking snapshots

1. To take a snapshot immediately, click **Take Snapshot** in the Manage backups and snapshots tab and then click **Yes** to confirm.

2. To delete a snapshot, select the snapshot from the snapshot list and click **Delete**.
3. When you are done making changes, click **OK**.

Exposing a snapshot

You can view a read-only copy of a snapshot of an Exchange storage group, SQL Server database, or user-defined application by exposing the snapshot on your HP All-in-One Storage System. Exposing a snapshot allows you to view the contents of a snapshot and selectively revert files.

NOTE:

A snapshot of a shared folder cannot be exposed using ASM. Use the Shadow Copy Client to view snapshots of shared folders from a client computer. Snapshots of a shared folder are stored on the same logical disk as the shared folder, in a protected system folder.

To expose a snapshot:

1. Navigate to the Manage Backups and Snapshots window.
2. Select an unexposed snapshot from the snapshot list.
3. Click **Expose**.
4. Enter the expose path on the application server where you will view the snapshot.

Unexposing a snapshot

After restoring from a snapshot, you may choose to unexpose a snapshot.

To unexpose a snapshot:

1. Navigate to the **Manage Backups and Snapshots** window.
2. Select an exposed snapshot from the snapshot list.
3. Click **Unexpose**.
4. Click **Yes** to confirm.

Reverting data to snapshots

ASM allows you to revert data stored on your HP All-in-One Storage System to a snapshot. This overwrites the existing data and reverts it to a past state.

NOTE:

Snapshots of shared folders cannot be reverted using ASM. To revert a shared folder to a past snapshot, use the Shadow Copy Client.

NOTE:

Snapshots of local storage applications can not be reverted using ASM as all data that is on the same volume as the application would also be reverted.

1. In the Manage Backups and Snapshots page, select a snapshot from the list.

NOTE:

To view the contents of a snapshot, expose it. See "Exposing a snapshot" on page 83 for more information.

2. Click **Revert**.
3. Click **Yes** to confirm.

Scheduling and running backups

- To schedule backups, see Scheduling backups on page 77 for more information.

Managing backups

After scheduling backups, you are able to manage backups for Exchange storage group, SQL Server database, user-defined application, or shared folders. Based on the backup features that have been configured, you have the following options:

- Run virtual library backup-After you have created a virtual library for a component, you are able to run a virtual library backup from this location.
- Run alternative location backup- If an alternative backup device has been assigned, you may run an alternative location backup from this page.
- Launch the restore wizard- Clicking on this wizard will taking you through the restore process, for either a virtual library backup or an alternative location backup.

To run a virtual library, alternative location backup or launch the restore wizard:

1. Navigate to the Data Protection page. See for more information.
2. Select **Manage backups and snapshots**.
3. Select the appropriate action.

Restoring data from backups

ASM allows you to restore data to your HP All-in-One Storage System from the latest backups created using Data Protector Express. You can choose to overwrite the existing data with the backup, or restore the backup to an unused space on your HP All-in-One Storage System so you can selectively overwrite existing data.

1. Click on **Manage backups and snapshots** in the Data Protection window.
2. Click **Launch restore wizard** to launch the wizard.
3. Open the **Selecting Restore Destination** page.

If you want to restore data using a backup other than the latest backup, see *Selecting files for restoring* of the *HP StorageWorks Data Protector Express Users Guide and Technical Reference* for more information.

Selecting the restore destination

1. Do one of the following:
   - Select **Overwrite Restore** to overwrite the existing data with the backup.
   - Select **Different Location Restore** to save the backup to a different location, and then enter the location (path) where you want the backup saved on your HP All-in-One Storage System. To browse for the location, click **Browse**.
2. Click **Next** to open the **Launch DPX** page (see Launching DPX).

Launching DPX

1. Click **Launch DPX** to launch Data Protector Express (see Using DPX to restore data).
2. After the restore is complete, click **Finish** to exit the wizard.

Using DPX to restore data

1. When the login window appears, do the following:
   a. Enter `localhost` in the **Host name** field.
   b. Enter `ASMbackup` in the **User name** field.

   △ CAUTION:

   The default password for ASMbackup is blank. It can be changed in the Command Line Interface (CLI).

   c. Click **OK**.
2. Click **Jobs and Media** in the Favorites pane, located on the left side of the main window.
3. Double-click **ASMbackup** on the right side of the main window.
4. Select the restore job for the application or shared folder whose data you want to restore.

   NOTE:

   To modify properites of the job, right-click the **Restore Job Properties**. For example, you may want to choose a different device from which to restore or select different version of files to restore. To restore version fo files other than the latest backup, refer to *Selecting Files and File Versions* in the *HP StorageWorks Data Protector Express Users Guide and Technical Reference*.
5. Right-click the restore job and click **Run** to perform the restore.
6. Click **Yes** to confirm the restore.

   To view the status of the restore job, click **Job Status** in the Favorites pane.
7. Exit Data Protector Express.

Setting the password for the ASMbackup user account

To set or change the ASMBackup user password:

1. Use the Command Line interface (CLI) found at `C:\Program Files\HP\HP All-in-One Storage Manager\hpkacli.exe`.

   The password may be set interactively, allowing the password characters to be masked, or it may be set with a single command.
2. Use the following command to display usage details:

   ```
   > hpkacli /?
   ```

To specify a password

1. Type the following:

   ```
   > hpkacli set password
   ```
2. This will bring up the following:

   ```
   Current password for ASMbackup:
   New password for ASMbackup:
   Confirm new password for ASMbackup:
   ```
3. If the current password for ASM backup is blank, press return when prompted. Otherwise, enter the current password.
4. Confirm the new password by typing in password again under Confirm new password.
5. The password has been set.

Using the Administrators' account to change the ASMbackup password

1. Type in the following:

   ```
   > hpkacli set password/admin
   ```
2. This will bring up the following:

   ```
   Password of Admin user:
   New password for ASMbackup:
   Confirm new password for ASMbackup:
   ```
3. Type the Data Protector Express admin password.
4. Type in the new password for the ASMbackup account.
5. Confirm the new password by typing it in again.
6. The password has been set.

Installing Data Protector Express on other devices

The Data Protector Express installation on the All-in-One System acts as the master server for a Data Protector Express Management Domain. If you wish to use the All-in-One system as a Disk-To-Disk (D2D) backup target for other client or machines, you may install Data Protector Express on those machines and join the management domain.

NOTE:

Installing Data Protector Express on other servers is not required to backup Exchange, SQL Server, or User-Defined applications, when those applications are hosted by All-in-One Storage Manager. The instructions provided here are only needed if a user wishes to use AiO as a backup target for additional user data in their environment.

The All-in-One storage system provides an ISO image at `c:\hpnas\components\dpx\iso` that may be used to install Data Protector Express on Windows or Linux. You can burn a CD or DVD from the ISO image, or mount the image on a file system using various available tools. As an alternative, you may also download and install Data Protector Express from http://www.hp.com

1. When installing Data Protector Express on another machine, select **Join an existing Data Protector Express domain**.
2. When prompted, provide the hostname or IP address of the All-in-One Storage System.

An unlimited number of client platforms such as Windows XP and Vista may be added to the Data Protector Express domain managed by the AiO system. Server platforms such as Windows Server 2003 will require one license per protected server. The following license is required for server platforms such as Windows Server 2003:**HP Data Protector Express Network Client Agent BB121AA**.

You may use ASM to create and manage storage for Data Protector Express virtual libraries on the AiO. You may then create backup jobs in Data Protector Express that use these virtual libraries as targets for Disk-to-Disk backups of your protected clients and servers. See "Using the Create a Virtual Library Wizard" on page 68 for more information.

NOTE:

When manually creating or modifying backup jobs that were not created by ASM, do not use the Data Protector Express ASMbackup account. It is recommended that you create other Data Protector Express user accounts as needed.

6 Managing storage

After an application is hosted or shared folder is created on your HP All-in-One Storage System using a storage-allocation wizard, you can manage its storage and data by:

- Increasing or reducing the allocated storage, page 89
- Changing the percent full warning threshold, page 90
- Removing application areas from view, page 91
- Changing permissions, names, descriptions, or paths of shared folders, page 91
- Deleting shared folders, page 92

Increasing or reducing the allocated storage

You can increase or reduce the storage allocated to an application component, user-defined application, or shared folder after storage is initially allocated and configured using a storage-allocation wizard.

Increasing the storage allocated requires ASM to grow the logical disk (increase the amount of hard drive space allocated to the logical disk) holding the data. Reducing the allocated storage does not reduce the size of the logical disk holding the data, because once hard drive space is allocated to a logical disk, it cannot be unallocated due to the configuration of hard drives.

NOTE:

Unallocated storage on a logical disk is re-allocated by ASM when new or additional storage is allocated to an application component or shared folder and the advanced configuration values selected for the storage matches those of the logical disk.

For example, if an application component or shared folder's allocated storage is increased, any unallocated space on the logical disk where it resides is used before the logical disk grows.

1. Select the application component, user-defined application, or shared folder in the content pane.
2. In the Actions pane, click **Allocate Space** to open the Allocate Space wizard.

3. Change the size value:
   - Highlight the storage size unit value and then enter a new value as necessary: megabytes (MB), gigabytes (GB), or terabytes (TB).
   - Highlight the storage size number value and enter a new value, or click the arrow buttons to change the value.

   The Size Range column shows the minimum and maximum storage space that can be allocated to an application component, user-defined application, or shared folder. Whenever you change the storage space allocated to an application component or change an advanced configuration setting for an application component, the maximum value for Size Range is recalculated for each application component shown.

NOTE:

To change the percent full warning threshold and/or enforce allocated limit (shared folders only) setting, click **Advanced**. See "Selecting advanced configuration settings" on page 71 for more information.

4. Click **Next** to open the Review Tasks Summary page (see "Reviewing task summary and scheduling tasks" on page 78).

Changing the percent full warning threshold

You can change the percent full warning threshold value for an application component, user-defined application, or shared folder after storage is initially allocated and configured using a storage-allocation wizard. See Setting a percent full warning threshold on page 74 for more information.

NOTE:

For shared folders, you can set an enforced limit (quota) for allocated storage, as well as a warning threshold. For more information, see Enforcing an allocated storage limit for shared folders and local storage applications on page 75.

To change the percent full warning threshold from the Properties window:

1. Select the application component, user-defined application, or shared folder in the content pane.
2. In the Actions pane, click **Properties**.
3. Click the **Warning Threshold** tab.
4. Change the percent full warning threshold value.
5. Click **OK**.

To change the percent full warning threshold using the Allocate Space Wizard:

1. Select the application component, user-defined application, or shared folder in the content pane.
2. In the Actions pane, click **Allocate Space**.
3. Click **Advanced**.
4. Change the percent full warning threshold value.
5. Click **Next** to open the Review Tasks Summary page (see "Reviewing task summary and scheduling tasks" on page 78).

Removing application areas from view

You can remove application components and user-defined applications from view on the ASM user interface. This allows you to remove storage information from the content pane pertaining to storage allocations lost due to hard drive failure or storage for an application component or user-defined application whose storage you plan to unhost.

Removing an application component or user-defined application from view does not unhost its storage. Its storage is still hosted on your HP All-in-One Storage System. To permanently remove storage from your All-in-One storage system, you must first remove the storage that is hosted by AiO. Depending on the type of storage, see http://h71028.www7.hp.com/ERC/downloads/4AA1-1026ENW.pdf for information on how to remove different types of storage.

NOTE:

If you remove an application component or user-defined application from view without unhosting the storage, your All-in-One Storage System will re-discover the applications immediately.

NOTE:

This action is not available for shared folders. Because ASM automatically discovers top-level shared folders on your HP All-in-One Storage System, the folder would just reappear after the next discovery process. A shared folder is automatically removed from view when it is removed from your HP All-in-One Storage System.

To remove an application component or user-defined application from view:

1. Permanently remove storage from your AiO, depending on the type of application. The application component will still remain in the content pane.
2. Select the application component or user-defined application to remove in the content pane.
3. In the Actions pane, click **Remove from View**.

   A confirmation dialog box opens.
4. Do one of the following:
   - Click **OK** to remove the item from view.
   - Click **Cancel** to cancel the action.

Changing permissions, names, descriptions, or paths of shared folders

ASM cannot be used to change permissions, names, descriptions, or paths of top-level or nested shared folders that reside on your HP All-in-One Storage System. Use Windows Explorer or the Shared Folder MMC snap-in to change permissions, names, descriptions, or paths of shared folders that reside on your HP All-in-One Storage System.

ASM automatically discovers and adopts any changes you make to the permissions, names, descriptions, or paths of shared folders using other applications. You do not have to make any changes in ASM to implement the changes. Click **Refresh** in the Actions pane (or perform any action in ASM) to update the ASM user interface to display your changes.

You will need to know the path of a shared folder to change its permissions, name, description, or path. To find the path, select the shared folder in the content pane and then click **Properties** in the Actions pane. The share path listed on the General tab is the path for the shared folder.

Deleting shared folders

ASM cannot be used to delete top-level or nested shared folders that reside on your HP All-in-One Storage System. Use Windows Explorer or the Shared Folder MMC snap-in to delete shared folders that reside on your HP All-in-One Storage System.

A shared folder is automatically removed from view on the ASM user interface when it is deleted from your HP All-in-One Storage System.

7 Monitoring storage

ASM provides storage-management functions so you can quickly view used and allocated storage, and percent full warning thresholds settings for application and shared folder storage on your HP All-in-One Storage System. You have a choice of these views for the content pane:

- Application View, page 93—Monitoring the overall used and allocated storage values for specific applications and shared folders (such as Exchange or SQL Server storage)
- Storage View, page 105—Monitoring the used and allocated storage values for the logical disks and volumes on your HP All-in-One Storage System that ASM created to host application storage and shared folders.
- Application Server View, page 108—Monitoring the application servers with storage hosted on your HP All-in-One Storage System.
- Storage Utilization View, page 110—Monitoring the allocated storage values for specific applications and the shared folders pool, the unallocated storage value, and the storage value for data not managed by ASM.

Views are selected from the Actions pane.

You can also quickly view storage status on the content pane. Status icons for warnings and critical conditions are displayed on top of icons in the content pane when storage status changes from OK to Warning or Critical. See "ASM alerts" on page 112 for more information on status icons.

NOTE:

Select an item in the content pane and then click **Properties** in the Actions pane to view any alerts for the item. See "ASM alerts" on page 112 for alert descriptions and troubleshooting information.

Application View

Application View displays the used and allocated storage space, and storage status of applications and shared folders hosted on your HP All-in-One Storage System in the content pane.

- In the Actions pane, select **Application View**.
- To view all the application storage and shared folders hosted on your HP All-in-One Storage System in the content pane, select **All** from the Filters drop-down menu, located at the top of the content pane. See Filters drop-down menu on page 57 for more information.

Application storage properties are displayed in order of hierarchy in an expandable and collapsible view.

Click the Expand tree icon next to each application to view the used and allocated storage properties for the hosted application components. Click the Collapse tree icon next to expanded applications to hide the application component storage properties.

To view all the storage properties for an item listed in the content pane, see Accessing application and shared folder properties.

Accessing application and shared folder properties

When Application View is selected in the Actions pane, you can view the storage status, alerts, and properties for the following:

- Applications
- Application component
- User-defined applications
- Shared folders pool
- Shared folders

Do one of the following:

- Select the item in the content pane and then click **Properties** in the Actions pane.
- Right-click the item in the content pane and select **Properties**.

NOTE:

ASM rolls up all status alerts to the highest level. For instance, if a top-level shared folder has surpassed its percent full warning threshold and exceeded its enforced allocated storage space, a warning message is shown in the shared folders pool. Likewise, if a critical status alert exists in an Exchange mail store, that alert is also shown in the status for the Exchange storage group.

Accessing properties for Exchange, Exchange storage group, and Exchange storage group components

ASM provides properties information for Exchange, Exchange storage group, and Exchange storage group components when Exchange storage is hosted on your HP All-in-One Storage System.

1. In the Actions pane, select **Application View**.
2. From the Filters drop-down menu, select **Exchange** or **All**.
3. To access Exchange:
   - Select **Exchange** in the content pane and then click **Properties** in the Actions pane.
   - Right-click **Exchange** in the content pane and select **Properties**.

To access Exchange Storage groups and components:

- Select any **Exchange storage group** or **Exchange storage group component** in the content pane and then click **Properties** in the Action pane.
- Right-click any Exchange storage group or component in the content pane and select Properties.

Properties window

ASM provides properties information for Exchange, Exchange storage groups, and components for storage hosted on your HP All-in-One Storage System. The following lists the tabs available in the properties window, and in parenthesis, if it applies to Exchange, Exchange storage groups, or Exchange storage group components.

- **General tab**—(Exchange, Exchange storage groups, and components) Displays the name of the application, the total capacity reserved for the application, and its operating status:

Table 21 Operating status: Exchange properties

Status indicator	Value
OK	Exchange is running and storage is online. No alerts.
Warning	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.
Critical	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.

Table 22 Details tab: Exchange storage group properties

Property	Value
Exchange Server	Name of server where Exchange storage is being hosted.
Exchange Version	Version of Exchange.
Days before log file removal	The number of days before log files are deleted from the server.
Directory Server	The domain controller used by the server.
Server Type	The type of Exchange installation: Front-end or Back-end. ASM can only host storage from Back-end Exchange servers, because Front-end Exchange installations do not actually store mailboxes and other Exchange data.
Clustered	Indicates whether the server that hosts SQL Server is part of a cluster.
Replication Type	Type of Exchange replication enabled.
LCR status	Indicates Exchange status for LCR.
LCR Copy	Indicates if Exchange component is the original or a copy.
LCR Log Folder Copy	Path to the LCR log file copies
LCR System Folder Copy	Path to LCR system file copies

- **Data Protection tab**—(Exchange storage groups, exchange storage group components) Allows you to schedule backups or run a backup of the storage group, or restore the storage group from a backup. It also allows you to schedule snapshots or take a snapshot of the storage group, expose a snapshot, or revert the storage group to a past snapshot. See "Data protection" on page 81 for more information.
- **Storage tab**—(Exchange storage group properties) Displays the storage group component's storage space, including allocated space, used space, free space, and the following storage allocation details:

Table 23 Storage tab: Exchange storage group component properties

Property	Value
Application Path	Path to the file directory on the server that hosts Exchange where the storage group component's data is saved by Exchange. The file directory is located on the volume created on the iSCSI LUN exported by ASM to the server that hosts Exchange.

Property	Value
Protocol	Communication protocol used to transfer data between the server that hosts Exchange (and the storage group component) and your HP All-in-One Storage System.
Application Server Host Name	Name of server that hosts Exchange and the storage group component.
Application Server Volume - Name	Name of the volume on the server that hosts Exchange to which Exchange saves the storage group component's data. The volume resides on the iSCSI LUN exported by ASM to the server that hosts Exchange.
Application Server Volume - Status	Status of the volume on the server that hosts Exchange where the storage group component is stored.
Application Server Volume - Exclusive Storage	Indicates if storage group component's storage is configured with exclusive storage. See Table 19 on page 72 for more information.
Application Server Volume - RAID Level	The RAID level to which the storage group component storage is configured. See Customizing RAID levels on page 73 for more information.
Application Server Volume - RAID Stripe Size	The RAID stripe size to which the storage group component's storage is configured. See Table 19 on page 72 for more information.
Application Server Volume - Read Cache	Speeds up reads when enabled. This setting is determined by the storage array, not ASM.
Application Server Volume - Write Cache	Speeds up writes when enabled. This setting is determined by the storage array, not ASM.
Application Server Volume - Number of Hot Spares	The number of hot spares with which the storage group component storage is configured. See Table 19 on page 72 for more information.
Application Server Volume - Mount Paths	Path the volume is mounted on, on the server that hosts Exchange. The volume is built on the iSCSI LUN exported by ASM to the server that hosts Exchange.

- **Warning Threshold tab**—(Exchange storage group components) Allows you to change the Percent Full Warning Threshold value for the storage group component. See Setting a percent full warning threshold on page 74 for more information.
- **Mail Store, Public Store, or Log tab**—(Exchange storage group components) One of these three tabs is available depending on whether the storage group component is a mail store, public store, or log.
  - **Mail Store tab**—Displays the status and properties of the mail store reported byt the Exchange server.

Table 24 Mail Store tab: Exchange storage group component properties

Value	Description
Mail Store Name	Name of storage group mail store.
Online	The storage group mail store is available for use.
Database File	Path to the file that stores all messages submitted through MAPI, as well as the database tables that define mailboxes, messages, folders, and attachments.

Value	Description
Streaming Database File (Exchange 2003 only)	Path to the file that stores Internet-formatted messages, such as native Multipurpose Internet Extensions (MIME) content.
Replication type	Indicates if LCR is being used.
LCR Status	Indicate Exchange warnings for LCR.
LCR Copy	Copy of the active/original exchange component.
LCR Database Copy File	Path to LCR mailstore copy

- **Public Store tab**—Displays the public store's free space and the following storage allocation details about the public store:

Table 25 Public Store tab: Exchange storage group component properties

Value	Description
Public Store Name	Name of storage group public store.
Online	The storage group public store is available for use.
Database File	Path to the file that stores all messages submitted through MAPI, as well as the database tables that define mailboxes, messages, folders, and attachments.
Streaming Database File (Exchange 2003 only)	Path to the file stores Internet-formatted messages, such as native Multipurpose Internet extensions (MIME) content.
Replication Type	Indicates if LCR is being used.
LCR Status	Indicate Exchange warnings for LCR.
LCR Copy	Copy of the active/original exchange component.
LCR Database Copy File	Path to the LCR public folder copy

- **Log tab**—Displays the log's free space and the following storage allocation details about the log:

Table 26 Log tab: Exchange storage group component properties

Value	Description
Path	Path to the log file.
Circular Logging	Indicates whether or not circular logging is enabled. If enabled, a new log entry will replace the oldest log entry when the size limit is reached.
Replication Type	Indicates if LCR is being used.
LCR Status	Indicate Exchange warnings for LCR.
LCR Copy	Copy of the active/original exchange component.
LCR Log Folder Copy	Path to the LCR log file copies

Value	Description
LCR System Folder Copy	Path to LCR system file copies

Accessing properties for shared folders

ASM provides properties information for shared folders pool and for any shared folder on your HP All-in-One Storage System. Using properties information, you can determine details about shared-folder status, including allocated space, and nested shares (if any), whether shared-folder storage is online or offline, and any warning or critical status indicators.

1. In the Actions pane, select **Application View**.
2. From the Filters drop-down menu, select **Shared Folders** or **All**.
3. Do one of the following:
   - Select **Shared Folders** in the content pane and then click **Properties** in the Actions pane.
   - Right-click **Shared Folders** in the content pane and select **Properties**.

- **General tab**— (Shared folders pool, shared folders) Displays the shared folder name, type of shared folder, share path on your HP All-in-One Storage System, share description, and the shared folder operating status:

Table 27 Operating status: Shared folder properties

Status indicator	Value
OK	The storage is online.
Warning	The storage has surpassed the percent full warning threshold. See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.
Critical	Shared folder storage has past the allocated storage limit and alerts are shown. See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.

- **Storage tab**—(Shared folders) Displays the shared folder storage space, including allocated space, used space, free space, and the following storage allocation details:

Table 28 Storage tab: Shared folder properties

Property	Value
Storage Server Host Name	Name of your HP All-in-One Storage System.
Storage Server Volume - Name	Name of the volume on your HP All-in-One Storage System where the shared folder is stored.
Storage Server Volume - Status	Status of the volume that holds the shared folder on your HP All-in-One Storage System.
Storage Server Volume - Exclusive Storage	Indicates if shared folder's storage is configured with exclusive storage. See Table 19 on page 72 for more information.
Storage Server Volume - RAID Level	The RAID level to which the shared folder's storage is configured. See Customizing RAID levels on page 73 for more information.

Property	Value
Storage Server Volume - RAID Stripe Size	The RAID stripe size to which the shared folder's storage is configured. See Table 19 on page 72 for more information.
Storage Server Volume - Read Cache	Speeds up reads when enabled. This setting is determined by the storage array, not ASM.
Storage Server Volume - Write Cache	Speeds up writes when enabled. This setting is determined by the storage array, not ASM.
Storage Server Volume - Number of Hot Spares	The number of hot spares with which the shared folder's storage is configured. See Table 19 on page 72 for more information.
Storage Server Volume - Mount Paths	Path to where the volume that holds the shared folder on your HP All-in-One Storage System is mounted.

- **Warning Threshold tab**—(Shared folders) Allows you to enable or disable the enforcement of the allocated space limit for the shared folder. See Enforcing an allocated storage limit for shared folders and local storage applications on page 75 for more information. Also, allows you to change the shared folder's percent full warning threshold value. See Setting a percent full warning threshold on page 74 for more information.
- **Nested Shares tab**—(Shared folders) Displays the list of nested file shares (if any) contained within the shared folder.
- **Data Protection tab**—(Shared folders) Allows you to schedule backups or run a backup of the shared folder, or restore the shared folder from a backup. It also allows you to schedule snapshots or take a snapshot of the shared folder. See "Selecting data protection" on page 76 for more information.

Accessing properties for SQL Server

ASM provides properties information for SQL Server when SQL Server storage is hosted on your HP All-in-One Storage System.

1. In the Actions pane, select **Application View**.
2. From the Filters drop-down menu, select **SQL Server** or **All**.
3. Do one of the following:
   - Select one of the following:**SQL Server, SQL Server database or a SQL Server database component** in the content pane and then click **Properties** in the Actions pane.
   - Right-click **SQL Server, SQL Server database or a SQL Server database component** in the content pane and select **Properties**.

Properties window

ASM provides properties information for the SQL server, databases and database components when SQL Server storage is hosted on your HP All-in-One Storage System. The following lists the tabs in the properties window, and in parenthesis, which applications are applicable: SQL Server, SQL Server databases or SQL Server database components.

- **General tab**—(SQL Server, SQL Server database, SQL Server database component) Displays the name of the application, the total capacity reserved for the application, and its operating status:

Table 29 Operating status: SQL Server properties

Status indicator	Value
OK	SQL Server is running and storage is online. No alerts.
Warning	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.
Critical	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.

- **Storage tab**—(SQL Server database component) Displays the database component's storage space, including allocated space, used space, free space, and the following storage allocation details:

Table 30 Storage tab: SQL Server database component properties

Property	Value
Application Path	Path to the file directory on the server that hosts SQL Server where the database component's data is saved by SQL Server. The file directory is located on the volume created on the iSCSI LUN exported by ASM to the server that hosts SQL Server.
Protocol	Communication protocol used to transfer data between the server that hosts SQL Server (and the database component) and your HP All-in-One Storage System.
Application Server Host Name	Name of server that hosts SQL Server and the database component.
Application Server Volume - Name	Name of the volume on the server that hosts SQL Server to which SQL Server saves the database component's data. The volume resides on the iSCSI LUN (logical disk) exported by ASM to the server that hosts SQL Server.
Application Server Volume - Status	Status of the volume on the server that hosts SQL Server where the database component is stored.
Application Server Volume - Exclusive Storage	Indicates if database component storage is configured with exclusive storage. See Table 19 on page 72 for more information.
Application Server Volume - RAID Level	The RAID level to which the database component storage is configured. See Customizing RAID levels on page 73 for more information.
Application Server Volume - RAID Stripe Size	The RAID stripe size to which the database component's storage is configured. See Table 19 on page 72 for more information.
Application Server Volume - Read Cache	Speeds up reads when enabled. This setting is determined by the storage array, not ASM.
Application Server Volume - Write Cache	Speeds up writes when enabled. This setting is determined by the storage array, not ASM.
Application Server Volume - Number of Hot Spares	The number of hot spares with which the database component storage is configured. See Table 19 on page 72 for more information.

Property	Value
Application Server Volume - Mount Paths	Path the volume is mounted on, on the server that hosts SQL Server. The volume is built on the iSCSI LUN exported by ASM to the server that hosts SQL Server.

- **Warning Threshold tab**—(SQL Server database component) Allows you to change the percent full warning threshold value for the database component. See Setting a percent full warning threshold on page 74 for more information.
- **Data File or Log tab**— (SQL Server database component) One of these two tabs is available depending on whether the database component is a data file or log.
- **Data File tab**—Displays the data file's free space and the following storage allocation details about the SQL Server data file:

Table 31 Data File tab: SQL Server database component properties

Value	Description
Data File Name	Name of database data file.
Filename	Relative path to where the database data file is stored on the server that hosts SQL Server.
File Group	File group of data file. This value is assigned by SQL Server.
Data File Space Available	Free storage space available for data file.

- **Log tab**—Displays the log file's free space and the following storage allocation details about the SQL Server log file.

Table 32 Log tab: SQL Server database component properties

Value	Description
Log Name	Name of database log file.
File Name	Relative path to where the database log file is stored on the server that hosts SQL Server.

- **Data Protection tab**—(SQL server database, SQL server database component) Allows you to schedule backups or run a backup of the database that owns the database component, or restore the database that owns the database component from a backup. It also allows you to schedule snapshots or take a snapshot of the database that owns the database component, expose a snapshot, or revert the database that owns the database component to a past snapshot. See "Data protection" on page 81 for more information.

Accessing properties for the user-defined applications

ASM provides properties information for the user-defined applications on your HP All-in-One Storage System. Using properties information, you can determine the status of all user-defined application areas monitored by ASM, and any warning or critical status indicators.

1. In the Actions pane, select **Application View**.
2. From the Filters drop-down menu, select **User-Defined** or **All**.

3. To select properties for the user-defined application pool:
   - Select **User-Defined** in the content pane and then click Properties in the Actions pane.

     or
   - Right-click **User-Defined** in the content pane and select **Properties**.

   For a user-defined application:
   - Select any user-defined application in the content pane and then click **Properties** in the Actions pane.

     or
   - Right-click any user-defined application in the content pane and select **Properties**.

Properties window

- **General tab**—Displays the user-defined application name, name of the application server that runs the user-defined application, and the application area status:

  Table 33 Operating status: User-defined application properties

Status indicator	Value
OK	Application storage is online. No alerts.
Warning	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.
Critical	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.

- **Storage tab**—Displays the user-defined application's storage space, including allocated space, used space, free space, and the following storage allocation details:

  Table 34 Storage tab: User-defined application properties

Property	Value
Application Path	Path to the file directory on the application server where the user-defined application data is saved by the user-defined application. The file directory is located on the volume created on the iSCSI LUN that was exported by ASM to the application server.
Protocol	Communication protocol used to transfer data between the server that hosts the user-defined application and your HP All-in-One Storage System.
Application Server Host Name	Name of server that hosts the user-defined application.
Application Server Volume - Name	Name of the volume on the application server to which the user-defined application saves its data. The volume resides on the iSCSI LUN (logical disk) exported by ASM to the application server.
Application Server Volume - Status	Status of the volume on the application server where the user-defined application data is stored.
Application Server Volume - Exclusive Storage	Indicates if user-defined application storage is configured with exclusive storage. See Table 19 on page 72 for more information.

Property	Value
Application Server Volume - RAID Level	The RAID level to which the user-defined application storage is configured. See Customizing RAID levels on page 73 for more information.
Application Server Volume - RAID Stripe Size	The RAID stripe size to which the user-defined application storage is configured. See Table 19 on page 72 for more information.
Application Server Volume - Read Cache	Speeds up reads when enabled. This setting is determined by the storage array, not ASM.
Application Server Volume - Write Cache	Speeds up writes when enabled. This setting is determined by the storage array, not ASM.
Application Server Volume - Number of Hot Spares	The number of hot spares with which the database component storage is configured. See Table 19 on page 72 for more information.
Application Server Volume - Mount Paths	Path the application server volume is mounted on. The volume is built on the iSCSI LUN exported by ASM to the application server.

- **Warning Threshold tab**—Allows you to change the percent full warning threshold value for the user-defined application. See Setting a percent full warning threshold on page 74 for more information.
- **Data Protection tab**—Allows you to schedule backups or run a backup of the user-defined application data, or restore the user-defined application data from a backup. It also allows you to schedule snapshots or take a snapshot of the user-defined application data, expose a snapshot, or revert the user-defined application data to a past snapshot. See "Data protection" on page 81 for more information.

Data Protection

Data Protection allows you to configure for virtual libraries and snapshots.

Properties window

ASM provides properties information on your HP All-in-One Storage System. The following lists the tabs available in the properties window for Data Protection.

Table 35 Operating status: Data Protection properties

Status indicator	Value
OK	Data Protection is running and storage is online. No alerts.
Warning	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.
Critical	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.

Table 36 Storage tab: Shared folder properties

Property	Value
Storage Server Host Name	Name of your HP All-in-One Storage System.

Property	Value
Storage Server Volume - Name	Name of the volume on your HP All-in-One Storage System where the shared folder is stored.
Storage Server Volume - Status	Status of the volume that holds the shared folder on your HP All-in-One Storage System.
Storage Server Volume - Exclusive Storage	Indicates if shared folder's storage is configured with exclusive storage. See Table 19 on page 72 for more information.
Storage Server Volume - RAID Level	The RAID level to which the shared folder's storage is configured. See Customizing RAID levels on page 73 for more information.
Storage Server Volume - RAID Stripe Size	The RAID stripe size to which the shared folder's storage is configured. See Table 19 on page 72 for more information.
Storage Server Volume - Read Cache	Speeds up reads when enabled. This setting is determined by the storage array, not ASM.
Storage Server Volume - Write Cache	Speeds up writes when enabled. This setting is determined by the storage array, not ASM.
Storage Server Volume - Number of Hot Spares	The number of hot spares with which the shared folder's storage is configured. See Table 19 on page 72 for more information.
Storage Server Volume - Mount Paths	Path to where the volume that holds the shared folder on your HP All-in-One Storage System is mounted.

- Warning Threshold- Allows you to change the percent full warning threshold value for the virtual library.

Table 37 Storage tab: Shared folder properties

Property	Value
Storage Server Host Name	Name of the host server for your virtual library.
Storage Server Volume - Name	Name of the volume on your HP All-in-One Storage System where the virtual library is stored.
Storage Server Volume - Status	Status of the volume that holds the virtual library on your HP All-in-One Storage System.
Storage Server Volume - Exclusive Storage	Indicates if the virtual library storage is configured with exclusive storage.
Storage Server Volume - RAID Level	The RAID level to which the virtual library's storage is configured. See Customizing RAID levels on page 73 for more information.
Storage Server Volume - RAID Stripe Size	The RAID stripe size to which the virtual library's storage is configured. See Table 19 on page 72 for more information.
Storage Server Volume - Read Cache	Speeds up reads when enabled. This setting is determined by the storage array, not ASM.
Storage Server Volume - Write Cache	Speeds up writes when enabled. This setting is determined by the storage array, not ASM.
Storage Server Volume - Number of Hot Spares	The number of hot spares with which the virtual library storage is configured.

Property	Value
Storage Server Volume - Mount Paths	Path to where the volume that holds the virtual library on your HP All-in-One Storage System is mounted.

Table 38 Virtual Library Properties

Property	Value
Device name	Name of device
Machine name	Name of machine hosting the virtual library
Device path	Location of device
Slot count	Number of slots used for a virtual library

Storage View

Storage View displays the used and allocated storage space of the storage areas (logical disks and volumes) on your HP All-in-One Storage System that were created by ASM to store application data and shared folders.

- In the Actions pane, select **Storage View**.
- To view the storage area properties for all applications and shared folders hosted on your HP All-in-One Storage System, select **All** from the Filters drop-down menu, located at the top of the content pane. See Filters drop-down menu on page 57 for more information.

Storage area properties are displayed in order of hierarchy in an expandable and collapsible view. For example, all the volumes on your HP All-in-One Storage System are displayed under the logical disks they reside on, and all the applications and shared folders hosted on your HP All-in-One Storage System are displayed under the volumes on which they are stored. Application components and individual shared folders are displayed under the application or shared folders pool to which they belong.

Click the Expand tree icon next to each logical disk name to view the volume's storage properties. Click the Collapse tree icon next to expanded logical disks to hide the volume's storage properties.

ASM assigns a drive letter to each volume on a logical disk. The drive letter can be viewed on the volume's Properties window. See
Accessing properties for HP All-in-One Storage System volumes on page 106 for more information.

NOTE:

A logical disk can only have one RAID configuration, so an application's components will reside on more than one logical disk if different RAID levels are selected for the application components using the storage-allocation wizard.

To view all the storage properties for an item listed in the content pane, see Accessing storage area properties.

Accessing storage area properties

When Storage View is selected in the Actions pane, you can view the storage status, alerts, and properties for the following storage areas on your HP All-in-One Storage System:

- Volumes
- Logical disks

Do one of the following:

- Select the item in the content pane and then click **Properties** in the Actions pane.
- Right-click the item in the content pane and select **Properties**.

Accessing properties for HP All-in-One Storage System volumes

ASM provides properties information for any volume on a logical disk on your HP All-in-One Storage System.

1. In the Actions pane, select **Storage View**.
2. Do one of the following:
   - Select any Volume (Vol) area in the content pane and then click **Properties** in the Actions pane.
   - Right-click any Volume (Vol) area in the content pane and select **Properties**.

Accessing properties for HP All-in-One Storage System logical disks

ASM provides properties information for the logical disks created on your HP All-in-One Storage System by ASM.

1. In the Actions pane, select **Storage View**.
2. Do one of the following:
   - Select any logical disk in the content pane and then click **Properties** in the Actions pane.
   - Right-click any logical disk in the content pane and select **Properties**.

Properties window

ASM provides properties information for any logical disks and for any logical disk created on your HP All-in-One Storage System.

General tab—Based on the application opened, logical disks or volumes, it will list the operating status for that application only.

Table 39 Operating status: General tab

Status indicator	Value
OK	The storage is online. No alerts.
Warning	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.
Critical	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.

Storage tab—Displays the unallocated space, used space, free space on the volume, and also details on your volume or logical disk properties, depending on the application open:

Table 40 Storage tab: HP All-in-One Storage System logical disk properties

Property	Value
System Name	Name the system uses to identify the logical disk.
Physical Disks	Globally unique identifier(s) of the hard drive(s) used by the logical disk for storage.
Exclusive Storage	Indicates if the logical disk is configured with exclusive storage. See Table 19 on page 72 for more information.
RAID Level	The RAID level to which the logical disk is configured. See Customizing RAID levels on page 73 for more information.
RAID Stripe Size	The RAID stripe size to which the logical disk is configured. See Table 19 on page 72 for more information.
Read Cache	Speeds up reads when enabled. This setting is determined by the storage array, not ASM.
Write Cache	Speeds up writes when enabled. This setting is determined by the storage array, not ASM.
Number of Hot Spares	The number of hot spares with which the logical disk is configured. See Table 19 on page 72 for more information.
Unmanaged Data	Space on the logical disk used to store data that is not managed by ASM.
Free Space	Unused storage space on the logical disk that is not allocated.

Table 41 Storage tab: HP All-in-One Storage System volume properties

Property	Value
Storage Server Host Name	Name of your HP All-in-One Storage System.
Storage Server Volume - Name	Name of the volume on your HP All-in-One Storage System.
Storage Server Volume - Status	Status of the volume on your HP All-in-One Storage System.
Storage Server Volume - Exclusive Storage	Indicates if volume is configured with exclusive storage. See Table 19 on page 72 for more information.
Storage Server Volume - RAID Level	The RAID level to which the volume is configured. See Customizing RAID levels on page 73 for more information.
Storage Server Volume - RAID Stripe Size	The RAID stripe size to which the volume is configured. See Table 19 on page 72 for more information.
Storage Server Volume - Read Cache	Speeds up reads when enabled. This setting is determined by the storage array, not ASM.
Storage Server Volume - Write Cache	Speeds up writes when enabled. This setting is determined by the storage array, not ASM.
Storage Server Volume - Number of Hot Spares	The number of hot spares with which the shared folder's storage is configured. See Table 19 on page 72 for more information.

Property	Value
Storage Server Volume - Mount Paths	Path on which the volume on your HP All-in-One Storage System is mounted.

- **Warning Threshold tab**—Allows you to change the percent full warning threshold value for the user-defined application.
- **Data Protection tab**—Allows you to schedule backups or run a backup of the user-defined application data, or restore the user-defined application data from a backup. It also allows you to schedule snapshots or take a snapshot of the user-defined application data, expose a snapshot, or revert the user-defined application data to a past snapshot.

Application Server View

Application Server View lists your HP All-in-One Storage System and the application servers with storage hosted on your HP All-in-One Storage System. Expand **HP All-in-One Storage System** to display the top-level shared folders on your HP All-in-One Storage System. Expand the application servers listed to display the application server volumes and the applications hosted on the volumes.

- In the Actions pane, select **Application Server View**.
- To view the properties for all application servers with storage hosted on your HP All-in-One Storage System, select **All** from the Filters drop-down menu, located at the top of the content pane. See Filters drop-down menu on page 57 for more information.

Application server properties are displayed in order of hierarchy in an expandable and collapsible view. For example, all the volumes created on the iSCSI LUNs (logical disk) exported by ASM to the application server are displayed under the application server, and all the application components hosted from the application server are displayed under the application server.

Click the Expand tree icon next to each application server to view the used and allocated storage properties for the volume and application components. Click the Collapse tree icon next to an expanded application server to hide the volume and application component storage properties.

To view all the storage properties for an item listed in the content pane, see Accessing application server properties.

Accessing application server properties

When Application Server View is selected in the Actions pane, you can view the storage status, alerts, and properties for the following:

- Volumes created on the iSCSI LUNs (logical disks) exported by ASM to the application servers
- Shared folders and application components (same information displayed on Application View)

Do one of the following:

- Select the item in the content pane and then click **Properties** in the Actions pane.
- Right-click the item in the content pane and select **Properties**.

See "Accessing application and shared folder properties" on page 94 for descriptions of shared folder and application component properties.

Accessing properties for application server volumes

ASM provides properties information for application server volumes created on the iSCSI LUNs exported by ASM to the application server.

1. In the Actions pane, select **Application Server View**.
2. Do one of the following:
   - Select an application server volume in the content pane and then click **Properties** in the Actions pane.
   - Right-click an application server volume in the content pane and select **Properties**.
3. Click one of the following tabs:
   - **General tab**—Displays the name of the volume on the application server, the volume type, and status:

     Table 42 Operating status: Application server volume properties

Status indicator	Value
OK	The storage is online.
Warning	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.
Critical	See the Alerts list for more information. See Table 45 on page 113 for alert descriptions.

   - **Storage tab**—Displays the unallocated space, used space, free space on the volume, and the following storage allocation details:

     Table 43 Storage tab: Application server volume properties

Property	Value
Application Server Host Name	Name of the application server where the volume resides.
Application Server Volume - Name	Name of the volume on the application server. Volume is located on the iSCSI LUN exported by ASM.
Application Server Volume - Status	Status of the volume on the application server.
Application Server Volume - Exclusive Storage	Indicates if the volume on the application server is configured with exclusive storage. See Table 19 on page 72 for more information.
Application Server Volume - RAID Level	The RAID level to which the volume on the application server is configured. See Customizing RAID levels on page 73 for more information.
Application Server Volume - RAID Stripe Size	The RAID stripe size to which the volume on the application server is configured. See Table 19 on page 72 for more information.
Application Server Volume - Read Cache	Speeds up reads when enabled. This setting is determined by the storage array, not ASM.
Application Server Volume - Write Cache	Speeds up writes when enabled. This setting is determined by the storage array, not ASM.
Application Server Volume - Number of Hot Spares	The number of hot spares with which the volume on the application server is configured. See Table 19 on page 72 for more information.
Application Server Volume - Mount Paths	Path the volume is mounted on.

Storage Utilization View

Storage Utilization View displays the allocated storage values for specific applications and the shared folders pool, the unallocated storage value, and the storage value for data not managed by ASM in a pie chart.

- In the Actions pane, select **Storage Utilization View**.

The storage value for each application hosted, the shared folders pool, unallocated storage, and data not managed by ASM is displayed according to its percentage of total capacity, using colors selected in the Color Options window (see Changing color settings on page 58).

The total capacity of your HP All-in-One Storage System is divided into the following areas:

- **Exchange**—Storage allocated to host Exchange storage group components.
- **Shared Folders**—Storage allocated to host shared folders.
- **SQL Server**—Storage allocated to host SQL Server database components.
- **User-defined**—Storage allocated to host user-defined applications.
- **Unmanaged**—Storage used by data that is not managed by ASM.

  The unmanaged value is the total storage being used to store data not managed by ASM, such as application or shared folder data no longer managed by ASM because the application components or shared folder was removed from view (see "Removing application areas from view" on page 91) and any other data saved on your HP All-in-One Storage System that is not managed by ASM.

- **Unallocated**—Unused storage that is not allocated.

  The unallocated space value is the total unused space on your HP All-in-One Storage System that has not been allocated to host application or shared folder storage. Unallocated storage includes raw (unconfigured) storage and unused configured storage (logical disks).

NOTE:

Logical disks (LUNs) being used to store application data or shared folders cannot be grown (increased in size) by ASM using space on unused logical disks (configured storage); they can only be grown using raw storage.

Unused logical disks are reallocated by ASM when an unhosted application component, shared folder, or user-defined application's storage is hosted using a storage-allocation wizard and the advanced configuration settings selected in the wizard match those of the unused logical disk. You can find the advanced configuration settings and capacities of unused (and used) logical disks on the Properties window for each logical disk (see Accessing properties for HP All-in-One Storage System logical disks on page 106).

8 Troubleshooting, servicing, and maintenance

Troubleshooting the storage system

Use the references and general guidelines in this section to troubleshoot your HP StorageWorks All-in-One Storage System.

Operating system problems and resolutions

Use the suggestions below to help resolve operating system issues.

Table 44 Operating system problems

Problem	Action
Operating system locks up	Scan for viruses with an updated virus scan utility.
General protection fault (GPF) occurs. This can occur when the Microsoft operating system terminates suddenly with an error, including, but not limited to: • Miscalculating the amount of RAM needed for an allocation • Transferring execution to a segment that is not executable • Writing to a read-only or a code segment • Loading a bad value into a segment register • Using a null pointer A GPF is immediately identifiable by a blue screen with white text, and the text may contain information that identifies the problem.	• Remove any newly installed software or hardware to verify that they are not the cause. • Boot the server in Safe Mode or the last known good configuration. If neither of these actions resolves the problem, contact an authorized service provider. For more information about debugging tools or specific GPF messages, see the Microsoft web site: http://www.microsoft.com/whdc/devtools/debugging/default.mspx.
Errors are displayed in the error log	Follow the information provided in the error log, and then see the operating system documentation.

Operating system updates

Use care when applying operating system updates (service packs, hotfixes, and patches). Before updating the operating system, read the release notes for each update. If you do not require specific fixes from the update, HP recommends that you do not apply the updates.

If you decide to apply an operating system update:

1. Perform a full system backup.
2. Apply the operating system update using the instructions provided.

3. Install the current drivers.

Application software problems

If your application software locks up, perform the following actions:

- Check the application log and operating system log for entries indicating why the software failed.
- Check for incompatibility with other software on the server.
- Check the support web site of the software vendor for known problems.
- Review the log files for changes made to the server that may have caused the problem.
- Scan the server for viruses with an updated virus scan utility.

SQL Server errors

Host a SQL Server Database Wizard authentication error

Problem: While using the Host a SQL Server Database Wizard, you receive an error message informing you that ASM cannot authenticate with the server that hosts SQL Server.

Solution: Each SQL Server license (instance) must have a login for the local user called `ASMUser` with the server role defined as System Administrators. This login is created during the installation of the ASM agent on the server that hosts SQL Server; however, if another SQL Server license is installed after the ASM agent is installed, this login will not be configured.

To fix this problem, you can remove the ASM agent from the server that hosts SQL Server, and then reinstall it following the instructions in the *HP StorageWorks All-in-One Storage System quick start instructions* (no information will be lost). Or, manually enter the login as follows:

1. Open SQL Server Enterprise Manager.
2. Connect to the server with SQL Server data you want to store on your HP All-in-One Storage System.
3. Select the Security Folder.
4. Select **Logins**.
5. Select **New Login**.
6. In the Name field, enter `ASMUser`.
7. In the Domain field, enter the domain name for the server that hosts SQL Server.
8. Select the **Server Roles** tab.
9. Select the **System Administrators** server role and click **OK**.

ASM alerts

ASM generates an alert whenever the status of an application area or storage area changes from OK to Warning or Critical. The alerts describe the condition that caused the storage status to change.

Alerts are displayed on the General tab of the Properties window.

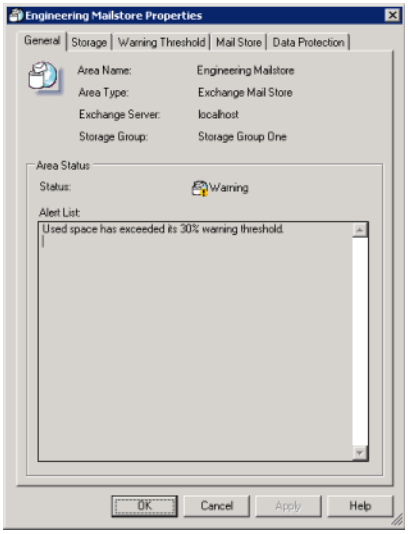


Figure 18 Example of alert

To view alerts:

- Select an item in the Content pane and click **Properties** in the Actions pane to view the alerts for the item selected.

Storage status is displayed as an icon when the storage status is Warning or Critical:

- In the Content pane on application, application component, or logical disk icons.
- In the Properties window on the General tab.

NOTE:

ASM rolls up any status alert to the highest level. For instance, if a shared folder has surpassed its percent full warning threshold and exceeded its allocated storage space, a warning icon is shown on the shared folders pool icon. Likewise, if a critical status exists in an Exchange mail store, the critical icon is also shown on the Exchange storage group icon.

Table 45 on page 113 lists all possible ASM alerts and provides descriptions, possible causes, and solutions for each alert.

Table 45 Alert descriptions

Object	Alert text	Description	Possible cause	Solution
Any application component, user-defined application, or shared folder	Directory size cannot be determined.	Used space cannot be determined.	Directory permission is preventing ASM from determining the used space or the logical disk has failed. An alert will be issued for the logical disk if it has failed.	Change directory permissions back to default permissions set by ASM. If the logical disk has failed, see "Recovering from logical disk failure" on page 117.
	Used space has exceeded its X% warning threshold.	Used space is about to surpass the percent full warning threshold (X%).	The percent of used space exceeds the percent full warning threshold or the logical disk has failed.	Increase the percent full warning threshold (see Setting a percent full warning threshold on page 74) or

Object	Alert text	Description	Possible cause	Solution
			An alert will be issued for the logical disk if it has failed.	increase the allocated storage (see "Increasing or reducing the allocated storage" on page 89).If the logical disk has failed, see "Recovering from logical disk failure" on page 117.
	Directory path cannot be found.	Allocated storage space cannot be located. Volume is intact.	Path assigned to allocated storage has been changed or the logical disk has failed. An alert will be issued for the logical disk if it has failed.	Change path to allocated storage back to path assigned by ASM.If the logical disk has failed, see "Recovering from logical disk failure" on page 117.
	Application data could not be found at path '*<path>*'.	A file cannot be found.	File has been moved or deleted.	Restore file or revert file using snapshot.
	Storage has reached its allocated space.	No more data can be saved to the allocated storage space. 100 percent of allocated storage is used.	Used storage has reached the total allocated space.	Increase the allocated space or delete data to reduce used storage. See "Increasing or reducing the allocated storage" on page 89 for more information.
	Storage not found for application area referencing host '*<server>*' path '*<path>*'.	The HP All-in-One Storage System volume that holds the application component's data can no longer be found at the mount path specified in the volume's storage properties.	The volume's mount path was changed using an application other than ASM.	Change the volume's mount path back to the path assigned by ASM.
Exchange storage group	This storage group could not be found on host '*<server>*' .	The storage group cannot be found on the server that hosts Exchange.	The storage group was deleted or renamed in Exchange, and storage is still hosted on your HP All-in-One Storage System.	Restore the storage group using Exchange or remove the storage for the storage group from view on the ASM user interface to stop receiving alerts.
Any Exchange storage group component	This storage group component could not be found on host '*<server>*' .	The storage group component cannot be found on the server that hosts Exchange.	The storage group component was deleted or renamed in Exchange, and storage is still hosted on your HP All-in-One Storage System.	Restore the storage group component using Exchange or remove the storage for the storage group component from view on the ASM user interface to stop receiving alerts.

Object	Alert text	Description	Possible cause	Solution
Exchange MailStore	This MailStore is offline.	Status of mail store is offline.	Administrator has placed mail store offline.	Return mail store to online.
Exchange PublicStore	This PublicStore is offline.	Status of public store is offline.	Administrator has placed public store offline.	Return public store to online.
SQL Server Database	This database is not in a functional state.	Database is offline.		
	This database could not be found on host '*<server>*' .		Database has been deleted or renamed.	Restore database or change its name back.
	This database is not attached.		This is an expected condition during a restore.	No action required.
SQL Server Data File	The location of this data file has changed.	The database exists but the data file cannot be found.	File has been moved or deleted.	Restore file or revert file using snapshot.
	This data file could not be found in the database '*<database>*' on host '*<server>*' .	The database exists but the data file cannot be found.	File has been moved or deleted.	Restore file or revert file using snapshot.
SQL Server Log	The location of this log has changed.	The database exists but the log file cannot be found.	File has been moved or deleted.	Restore file or revert file using snapshot.
	This log could not be found in the database '*<database>*' on host '*<server>*' .	The database exists but the log file cannot be found.	File has been moved or deleted.	Restore file or revert file using snapshot.
Logical Disk	Health: Rebuilding	Hard drive was replaced. Resyncing mirror on new hard drive if logical disk is RAID 1 or RAID 1+0(10). Rebuilding parity on new hard drive if logical disk is RAID 5 or RAID 6.	Hard drive was replaced.	No action required.

Object	Alert text	Description	Possible cause	Solution
	Health: Failing but still working	A hard drive is failing but still working.	Hard drive is failing.	Replace failing hard drive now (optional) or replace hard drive after it fails.
	Health: Failing redundancy but one mirror still working	Logical disk is configured as RAID 1 or RAID 1+0(10). One of the pair of mirrored hard drives is failing but the other hard drive is still working.	Hard drive is failing.	Replace failing hard drive now (optional) or replace hard drive after it fails.
	Health: Failed redundancy but one mirror still working	Logical disk is configured as RAID 1 or RAID 1+0(10). One of the pair of mirrored hard drives has failed but the other hard drive is still working.	Hard drive has failed.	Replace failed hard drive immediately to restore redundancy.
	Health: Failed redundancy, the last mirror is failing	Logical disk is configured as RAID 1 or RAID 1+0(10). One of the pair of mirrored hard drives has failed and the other hard drive is failing.	Hard drive has failed and another hard drive is failing.	Replace failed hard drive immediately to restore redundancy. If second hard drive fails before first is replaced, the logical disk and data on the logical disk will be lost.
	Health: Failed	Logical disk has failed.	Hard drive(s) with storage allocated to the logical disk have failed. The logical disk cannot be rebuilt. The logical disk and data on the logical disk are lost.	Replace the failed hard drives. Allocate new storage to replace lost storage. Restore data to allocated space using backups if available.
	Transition state: Extending	The logical disk is growing. Performance is degraded. Reads and writes can still be performed to logical disk.	ASM is growing a logical disk (LUN) to allocate new or more storage to an application component, user-defined application, or shared folder.	No action is required.
	Transition state: Reconfiguring	The logical disk is being reconfigured.	Configuration changes are being made to the logical disk by an application other than ASM.	No action is required.

Object	Alert text	Description	Possible cause	Solution
	Status: Not ready	Logical disk not usable while an operation is being performed.	Operation is being performed that prevents logical disk from being used.	No action is required.
	Status: Offline	Logical disk is not usable.	Administrator has taken logical disk offline.	Return the logical disk to online.
	Status: Failed	Logical disk is not usable.	Hardware failure has occurred.	See array controller documentation for more information.

Recovering from logical disk failure

Application component or shared folder data stored on a logical disk that failed is lost. To recover the data and reallocate storage on your HP All-in-One Storage System, replace any failed hard drives, allocate new storage on your HP All-in-One Storage System using a storage-allocation wizard to replace the lost storage, and then restore the data to the new allocated storage using a backup (see "Restoring data from backups" on page 84).

NOTE:

Snapshots cannot be used to recover data lost as a result of logical disk failure. Snapshots of Exchange storage groups, SQL Server databases, user-defined applications, and shared folders are stored on the same logical disks as the original data, and therefore are also lost.

Maintenance updates

Regular updates to the storage system are supplied on the HP All-in-One Storage System Service Release DVD. The Service Release DVD can be obtained at http://www.software.hp.com.

Individual updates for each product are available for download from the HP Support web site at http://h18023.www1.hp.com/support/selfrepair/na/replace_part.asp.

System updates

System updates to the hardware (BIOS, firmware, drivers), critical updates, and hotfixes for the operating system and other related software updates are bundled on the Service Release DVD.

Troubleshooting resources

HP web site

Troubleshooting tools and information, as well as the latest drivers and flash ROM images, are available at http://www.hp.com.

Storage system documentation

Storage system documentation is the set of documents provided with a storage system. Most storage system documents are available as a PDF file or a link on the documentation CD. Storage system documentation can be accessed from http://www.hp.com/support/manuals). Under the storage section, click **Disk Storage Systems** and then select your product.

Additional documentation can also be found on the inside of the access panel of certain system models.

Subscriber's Choice

HP Subscriber's Choice is a customizable subscription sign-up service that customers use to receive personalized e-mail product tips, feature articles, driver and support alerts, or other notifications.

To create a profile and select notifications, see http://www.hp.com/go/subscriberschoice.

White papers

White papers are electronic documents on complex technical topics. Some white papers contain in-depth details and procedures. Topics include HP products, HP technology, operating systems, networking products, and performance issues. See the HP Business Support Center at http://www.hp.com/go/bizsupport.

Firmware updates

Firmware is software that is stored in Read-Only Memory (ROM). Firmware is responsible for the behavior of the system when it is first switched on and for passing control of the server to the operating system. When referring to the firmware on the system board of the server, it is called the System ROM or the BIOS. When referring to the firmware on another piece of hardware configured in the server, it is called Option ROM. These systems have hard drives and Smart Array Controller options that have firmware that can be updated.

It is important to update the firmware (also called "flashing the ROM") as part of regular server maintenance. In addition, checking for specific firmware updates in between regular updates helps to keep the server performing optimally. HP recommends checking for a firmware update before sending a part back to HP for replacement.

Apply the latest firmware and software updates using the HP ProLiant Storage Server Service Release DVD. The DVD provides software updates, upgrades, and enhancements for the storage system. The Service Release can be ordered without cost from http://software.hp.com. On the web site, select the "Storage and NAS" category. The latest service release version appears in the list of available software.

WEBES (Web Based Enterprise Services)

WEBES is a tool suite aimed at preventing or reducing your system's down time. The tool suite has the following components:

- CCAT (Computer Crash Analysis Tool)
- SEA (System Event Analyzer)

If you have a warranty or service contract with HP you are entitled to these tools free of charge. You must, however, upgrade the tools at least once a year, because the software expires after one year. For more information about WEBES, see http://h18023.www1.hp.com/support/svctools/webes/.

To install WEBES on your storage system, run the setup executable located in the `C:\hpnas\Components\WEBES` folder.

Certificate of Authenticity

The Certificate of Authenticity (COA) label is used to:

- Upgrade the factory-installed operating system using the Microsoft Upgrade program for license validation.
- Reinstall the operating system because of a failure that has permanently disabled it.

The COA label location varies by server model. On rack-mounted server models, the COA label is located either on the front section of the right panel or on the right front corner of the top panel. On tower models, the COA label is located toward the rear of the top panel of the server.

9 System recovery

This chapter describes how to use the Recovery DVD that is provided with your All-in-One Storage System.

The System Recovery DVD

The *HP StorageWorks All-in-One Storage System Recovery DVD* that is provided with your storage system allows you to install an image or recover from a catastrophic failure.

You may boot from the DVD and restore the system to the factory condition at any time. This allows you to recover the system if all other means to boot the system fails.

While the recovery process makes every attempt to preserve the existing data volumes, you should have a backup of your data if at all possible before recovering the system.

To restore a factory image

1. Insert the System Recovery DVD. The main window appears.
2. Choose **Restore Factory Image**.

Systems with a DON'T ERASE partition

The DON'T ERASE logical disk supports the restoration process only and does not host a secondary operating system. Be sure to back up your user data, and then use the Recovery and Installation DVD to restore the system to the factory state.

Managing disks after a restoration

After a system has been restored, drive letters may be assigned to the wrong volume. Windows Storage Server 2003 assigns drive letters after the restoration in the order of discovery. To help maintain drive letter information, placing the drive letter into a volume label is recommended. To change the drive letters to the appropriate one, go into Disk Management and perform the following steps for each volume:

1. Right-click the volume that needs to be changed.
2. Select **Change drive Letter and Paths**.
3. In the **Change drive Letter and Paths** dialog box, select **Change**.
4. Select the appropriate drive letter an click **OK**.
5. Click **Yes** to confirm the drive letter change.
6. Click **Yes** to continue. If the old drive letter needs to be reused, reboot the system after clicking Yes.

A File server management

This chapter begins by identifying new or improved file services in Windows Storage Server 2003 R2. The remainder of the chapter describes the many tasks and utilities that play a role in file server management.

New or improved file services features in Windows Storage Server 2003 R2

Storage Manager for SANs

The Storage Manager for SANs (also called Simple SAN) snap-in enables you to create and manage the LUNs that are used to allocate space on storage arrays. Storage Manager for SANs can be used on SANs that support Virtual Disk Server (VDS). It can be used in both Fibre Channel and iSCSI environments.

For more information on Storage Manager for SANs, see the online help. A Microsoft document titled *Storage Management in Windows Storage Server 2003 R2: File Server Resource Manager and Storage Manager for Storage Area Networks* is available at http://download.microsoft.com/download/7/4/7/7472bf9b-3023-48b7-87be-d2cedc38f15a/WS03R2_Storage_Management.doc.

NOTE:

Storage Manager for SANs is only available on Standard and Enterprise editions of Windows Storage Server 2003 R2.

Single Instance Storage

Single Instance Storage (SIS) provides a copy-on-write link between multiple files. Disk space is recovered by reducing the amount of redundant data stored on a server. If a user has two files sharing disk storage by using SIS, and someone modifies one of the files, users of the other files do not see the changes. The underlying shared disk storage that backs SIS links is maintained by the system and is only deleted if all the SIS links pointing to it are deleted. SIS automatically determines that two or more files have the same content and links them together.

NOTE:

Single Instance Storage is only available on Standard and Enterprise editions of Windows Storage Server 2003 R2.

Search enhancements

The Indexing service is tuned for additional indexing and query performance. Prior to the R2 release, if the Indexing service on a Windows Storage Server was not entirely up-to-date, the client-side search engine needed to "walk through" all the files within the scope of the search on the server. With the performance tuning in R2, the Indexing service no longer needs to be entirely up-to-date.

File Server Resource Manager

File Server Resource Manager is a suite of tools that allows administrators to understand, control, and manage the quantity and type of data stored on their servers. By using File Server Resource Manager, administrators can place quotas on volumes, actively screen files and folders, and generate comprehensive storage reports.

By using File Server Resource Manager, you can perform the following tasks:

- Create quotas to limit the space allowed for a volume or folder and to generate notifications when the quota limits are approached and exceeded.
- Create file screens to screen the files that users can save on volumes and in folders and to send notifications when users attempt to save blocked files.
- Schedule periodic storage reports that allow users to identify trends in disk usage and to monitor attempts to save unauthorized files, or generate the reports on demand.

Windows SharePoint Services

Windows SharePoint Services is an integrated set of collaboration and communication services designed to connect people, information, processes, and systems, both within and beyond the organization firewall.

NOTE:

Windows SharePoint Services is only available on Standard and Enterprise editions of Windows Storage Server 2003 R2.

HP All-in-One Management Console

The HP All-in-One Management Console is a user interface in Windows Storage Server 2003 R2 that provides one place to manage files or print serving components. The console is accessible using Remote Desktop or a web browser.

The Storage Management page provides a portal to:

- File Server Resource Manager
- DFS Management
- Disk and Volume Management
- Indexing Service
- MSNFS (under Share folder)
- Cluster Management (under "Utilities")

The Share Folder Management page provides a portal to Shared Folders, consisting of:

- Shares

- Sessions
- Open Files

File services management

Configurable and pre-configured storage

Certain storage systems ship with storage configured only for the operating system. The administrator must configure data storage for the storage system. Other storage systems ship with pre-configured storage for data. Depending on the type of storage system purchased, additional storage configuration is required.

Configuring additional storage involves creating arrays, logical disks, and volumes. Table 46 shows the general task areas to be performed as well as the utilities needed to configure storage for an HP Smart Array-based storage system.

Table 46 Tasks and utilities needed for storage system configuration

Task	Storage management utility
Create disk arrays	HP Array Configuration Utility or Storage Manager
Create logical disks from the array space	HP Array Configuration Utility or Storage Manager
Verify newly created logical disks	Windows Disk Management
Create a volume on the new logical disk	Windows Disk Management

NOTE:

The type of configuration may not apply to all supported storage components and serves only as an example providing basic guidance.

- Create disk arrays—On storage systems with configurable storage, physical disks can be arranged as RAID arrays for fault tolerance and enhanced performance, and then segmented into logical disks of appropriate sizes for particular storage needs. These logical disks then become the volumes that appear as drives on the storage system.

CAUTION:

The first two logical drives are configured for the storage system operating system and should not be altered in any manner.

The fault tolerance level depends on the amount of disks selected when the array was created. A minimum of two disks is required for RAID 0+1 configuration, three disks for a RAID 5 configuration, and four disks for a RAID 6 (ADG) configuration.

- Create logical disks from the array space—Select the desired fault tolerance, stripe size, and size of the logical disk.
- Verify newly created logical disks—Verify that disks matching the newly created sizes are displayed.
- Create a volume on the new logical disk—Select a drive letter and enter a volume label, volume size, allocation unit size, and mount point (if desired).

NOTE:

Do not tamper with the "DON'T ERASE" or local C: volume. These are reserved volumes and must be maintained as they exist.

Storage management utilities

The storage management utilities pre-installed on the storage system include the HP Array Configuration Utility (ACU).

Array management utilities

Storage devices for RAID arrays and LUNs are created and managed using the array management utilities mentioned previously. For HP Smart Arrays use the ACU.

NOTE:

The ACU is used to configure and manage array-based storage. You need administrator or root privileges to run the ACU.

Array Configuration Utility

The HP ACU supports the Smart Array controllers and SCSI hard drives installed on the storage system.

To open the ACU from the storage system desktop:

NOTE:

If this is the first time that the ACU is being run, you will be prompted to select the Execution Mode for ACU. Selecting Local Application Mode allows you to run the ACU from a Remote Desktop, Remote Console, or storage system web access modes. Remote Service Mode allows you to access the ACU from a remote browser.

1. Select **Start > Programs > HP Management Tools > Array Configuration Utility**.
2. If the Execution Mode for ACU is set to Remote Mode, log in to the HP System Management Homepage. The default user name is **administrator** and the default password is **hpinvent**.

To open the ACU in browser mode:

NOTE:

Confirm that the ACU Extension Mode is set to remote service.

1. Open a browser and enter the server name or IP address of the destination server. For example, `http://servername:2301` or `http://192.0.0.1:2301`.
2. Log in to the HP System Management Homepage. The default user name is **administrator** and the default password is **hpinvent**.

3. Click **Array Configuration Utility** on the left side of the window. The ACU opens and identifies the controllers that are connected to the system.

Some ACU guidelines to consider:

- Do not modify the first two logical drives of the storage system; they are configured for the storage system operating system.
- Spanning more than 14 disks with a RAID 5 volume is not recommended.
- Designate spares for RAID sets to provide greater protection against failures.
- RAID sets cannot span controllers.
- A single array can contain multiple logical drives of varying RAID settings.
- Extending and expanding arrays and logical drives is supported.

The *HP Array Configuration Utility User Guide* is available for download at http://www.hp.com/support/manuals.

Disk Management utility

The Disk Management tool is a system utility for managing hard disks and the volumes, or partitions, that they contain. Disk Management is used to initialize disks, create volumes, format volumes with the FAT, FAT32, or NTFS file systems, and create fault-tolerant disk systems. Most disk-related tasks can be performed in Disk Management without restarting the system or interrupting users. Most configuration changes take effect immediately. A complete online help facility is provided with the Disk Management utility for assistance in using the product.

NOTE:

- When the Disk Management utility is accessed through a Remote Desktop connection this connection can only be used to manage disks and volumes on the server. Using the Remote Desktop connection for other operations during an open session closes the session.
- When closing Disk Management through a Remote Desktop connection, it may take a few moments for the remote session to log off.

Guidelines for managing disks and volumes

When managing disks and volumes:

- Do not alter the operating system disk labeled Local Disk C: or Primary OS C:.
- Do not alter the disk labeled “DON'T ERASE.”
- HP does not recommend spanning array controllers with dynamic volumes. The use of software RAID-based dynamic volumes is not recommended. Use the array controller instead; it is more efficient.
- Use meaningful volume labels with the intended drive letter embedded in the volume label, if possible. (For example, volume e: might be named “Disk E:.”) Volume labels often serve as the only means of identification.
- Record all volume labels and drive letters in case the system needs to be restored.
- When managing basic disks, only the last partition on the disk can be extended unless the disk is changed to dynamic.
- Basic disks can be converted to dynamic, but cannot be converted back to basic without deleting all data on the disk.

- Basic disks can contain up to four primary partitions (or three primary partitions and one extended partition).
- Format drives with a 16 K allocation size for best support of shadow copies, performance, and defragmentation.
- NTFS formatted drives are recommended, because they provide the greatest level of support for shadow copies, encryption, and compression.
- Only basic disks can be formatted as FAT or FAT32.
- Read the online Disk Management help found in the utility.

Scheduling defragmentation

Defragmentation is the process of analyzing local volumes and consolidating fragmented files and folders so that each occupies a single, contiguous space on the volume. This improves file system performance. Because defragmentation consolidates files and folders, it also consolidates the free space on a volume. This reduces the likelihood that new files will be fragmented.

Defragmentation for a volume can be scheduled to occur automatically at convenient times. Defragmentation can also be done once, or on a recurring basis.

NOTE:

Scheduling defragmentation to run no later than a specific time prevents the defragmentation process from running later than that time. If the defragmentation process is running when the time is reached, the process is stopped. This setting is useful to ensure that the defragmentation process ends before the demand for server access is likely to increase.

If defragmenting volumes on which shadow copies are enabled, use a cluster (or allocation unit) size of 16 KB or larger during the format. Otherwise defragmentation registers as a change by the Shadow Copy process. This increase in the number of changes forces Shadow Copy to delete snapshots as the limit for the cache file is reached.

CAUTION:

Allocation unit size cannot be altered without reformatting the drive. Data on a reformatted drive cannot be recovered.

For more information about disk defragmentation, read the online help.

Disk quotas

Disk quotas track and control disk space use in volumes.

NOTE:

To limit the size of a folder or share, see "Quota management" on page 152 .

Configure the volumes on the server to perform the following tasks:

- Prevent further disk space use and log an event when a user exceeds a specified disk space limit.
- Log an event when a user exceeds a specified disk space warning level.

When enabling disk quotas, it is possible to set both the disk quota limit and the disk quota warning level. The disk quota limit specifies the amount of disk space a user is allowed to use. The warning level specifies the point at which a user is nearing his or her quota limit. For example, a user's disk quota limit can be set to 50 megabytes (MB), and the disk quota warning level to 45 MB. In this case, the user can store no more than 50 MB on the volume. If the user stores more than 45 MB on the volume, the disk quota system logs a system event.

In addition, it is possible to specify that users can exceed their quota limit. Enabling quotas and not limiting disk space use is useful to still allow users access to a volume, but track disk space use on a per-user basis. It is also possible to specify whether or not to log an event when users exceed either their quota warning level or their quota limit.

When enabling disk quotas for a volume, volume usage is automatically tracked from that point forward, but existing volume users have no disk quotas applied to them. Apply disk quotas to existing volume users by adding new quota entries on the Quota Entries page.

NOTE:

When enabling disk quotas on a volume, any users with write access to the volume who have not exceeded their quota limit can store data on the volume. The first time a user writes data to a quota-enabled volume, default values for disk space limit and warning level are automatically assigned by the quota system.

For more information about disk quotas, read the online help.

Adding storage

Expansion is the process of adding physical disks to an array that has already been configured. Extension is the process of adding new storage space to an existing logical drive on the same array, usually after the array has been expanded.

Storage growth may occur in three forms:

- Extend unallocated space from the original logical disks or LUNs.
- Alter LUNs to contain additional storage.
- Add new LUNs to the system.

The additional space is then extended through a variety of means, depending on which type of disk structure is in use.

Expanding storage

Expansion is the process of adding physical disks to an array that has already been configured. The logical drives (or volumes) that exist in the array before the expansion takes place are unchanged, because only the amount of free space in the array changes. The expansion process is entirely independent of the operating system.

NOTE:

See your storage array hardware user documentation for further details about expanding storage on the array.

Extending storage using Windows Storage Utilities

Volume extension grows the storage space of a logical drive. During this process, the administrator adds new storage space to an existing logical drive on the same array, usually after the array has been expanded. An administrator may have gained this new storage space by either expansion or by deleting another logical drive on the same array. Unlike drive expansion, the operating system must be aware of changes to the logical drive size.

You extend a volume to:

- Increase raw data storage
- Improve performance by increasing the number of spindles in a logical drive volume
- Change fault-tolerance (RAID) configurations

For more information about RAID levels, see the *Smart Array Controller User Guide*, or the document titled *Assessing RAID ADG vs. RAID 5 vs. RAID 1+0*. Both are available at the Smart Array controller web page or at http://h18000.www1.hp.com/products/servers/proliantstorage/arraycontrollers/documentation.html.

Extend volumes using Disk Management

The Disk Management snap-in provides management of hard disks, volumes or partitions. It can be used to extend a dynamic volume only.

NOTE:

Disk Management cannot be used to extend basic disk partitions.

Guidelines for extending a dynamic volume:

- Use the Disk Management utility.
- You can extend a volume only if it does not have a file system or if it is formatted NTFS.
- You cannot extend volumes formatted using FAT or FAT32.
- You cannot extend striped volumes, mirrored volumes, or RAID 5 volumes.

For more information, see the Disk Management online help.

Expanding storage using the Array Configuration Utility

The Array Configuration Utility enables online capacity expansion of the array and logical drive for specific MSA storage arrays, such as the MSA1000 and MSA1500. For more information, use the ACU online help, or the procedures to “Expand Array” in the *HP Array Configuration Utility User Guide*

Expand logical drive

This option in the ACU increases the storage capacity of a logical drive by adding unused space on an array to the logical drive on the same array. The unused space is obtained either by expanding an array or by deleting another logical drive on the same array. For more information, use the ACU online help, or the “Extend logical drive” procedure in the *Array Configuration Utility User Guide*

Volume shadow copies

The Volume Shadow Copy Service provides an infrastructure for creating point-in-time snapshots (shadow copies) of volumes. Shadow Copy supports 64 shadow copies per volume.

A shadow copy contains previous versions of the files or folders contained on a volume at a specific point in time. While the shadow copy mechanism is managed at the server, previous versions of files and folders are only available over the network from clients, and are seen on a per folder or file level, and not as an entire volume.

The shadow copy feature uses data blocks. As changes are made to the file system, the Shadow Copy Service copies the original blocks to a special cache file, to maintain a consistent view of the file at a particular point in time. Because the snapshot only contains a subset of the original blocks, the cache file is typically smaller than the original volume. In the snapshot's original form, it takes up no space because blocks are not moved until an update to the disk occurs.

By using shadow copies, a storage system can maintain a set of previous versions of all files on the selected volumes. End users access the file or folder by using a separate client add-on program, which enables them to view the file in Windows Explorer. Accessing previous versions of files, or shadow copies, enables users to:

- Recover files that were accidentally deleted. Previous versions can be opened and copied to a safe location.
- Recover from accidentally overwriting a file. A previous version of that file can be accessed.
- Compare several versions of a file while working. Use previous versions to compare changes between two versions of a file.

Shadow copies cannot replace the current backup, archive, or business recovery system, but they can help to simplify restore procedures. Because a snapshot only contains a portion of the original data blocks, shadow copies can not protect against data loss due to media failures. However, the strength of snapshots is the ability to instantly recover data from shadow copies, reducing the number of times needed to restore data from tape.

Shadow copy planning

Before setup is initiated on the server and the client interface is made available to end users, consider the following:

- From what volume will shadow copies be taken?
- How much disk space should be allocated for shadow copies?
- Will separate disks be used to store shadow copies?
- How frequently will shadow copies be made?

Identifying the volume

Shadow copies are taken for a complete volume, but not for a specific directory. Shadow copies work best when the server stores user files, such as documents, spreadsheets, presentations, graphics, or database files.

NOTE:

Shadow copies should not be used to provide access to previous versions of application or e-mail databases.

Shadow copies are designed for volumes that store user data such as home directories and My Documents folders that are redirected by using Group Policy or other shared folders in which users store data.

Shadow copies work with compressed or encrypted files and retain whatever permissions were set on the files when the shadow copies were taken. For example, if a user is denied permission to read a file, that user would not be able to restore a previous version of the file, or be able to read the file after it has been restored.

Although shadow copies are taken for an entire volume, users must use shared folders to access shadow copies. Administrators on the local server must also specify the `\\servername\sharename` path to access shadow copies. If administrators or end users want to access a previous version of a file that does not reside in a shared folder, the administrator must first share the folder.

NOTE:

Shadow copies are available only on NTFS, not FAT or FAT32 volumes.

Files or folders that are recorded by using Shadow Copy appear static, even though the original data is changing.

Allocating disk space

When determining the amount of space to allocate for storing shadow copies, consider both the number and size of files that are being copied, as well as the frequency of changes between copies. For example, 100 files that only change monthly require less storage space than 10 files that change daily. If the frequency of changes to each file is greater than the amount of space allocated to storing shadow copies, no shadow copy is created.

Administrators should also consider user expectations of how many versions they will want to have available. End users might expect only a single shadow copy to be available, or they might expect three days or three weeks worth of shadow copies. The more shadow copies users expect, the more storage space administrators must allocate for storing them.

Setting the limit too low also affects backup programs that use shadow copy technology because these programs are also limited to using the amount of disk space specified by administrators.

NOTE:

Regardless of the volume space that is allocated for shadow copies, there is a maximum of 64 shadow copies for any volume. When the 65th shadow copy is taken, the oldest shadow copy is purged.

The minimum amount of storage space that can be specified is 350 megabytes (MB). The default storage size is 10 percent of the source volume (the volume being copied). If the shadow copies are stored on a separate volume, change the default to reflect the space available on the *storage* volume instead of the *source* volume. Remember that when the storage limit is reached, older versions of the shadow copies are deleted and cannot be restored.

CAUTION:

To change the storage volume, shadow copies must be deleted. The existing file change history that is kept on the original storage volume is lost. To avoid this problem, verify that the storage volume that is initially selected is large enough.

Identifying the storage area

To store the shadow copies of another volume on the same file server, a volume can be dedicated on separate disks. For example, if user files are stored on `H:\`, another volume such as `S:\` can be used to store the shadow copies. Using a separate volume on separate disks provides better performance and is recommended for heavily used storage systems.

If a separate volume will be used for the storage area (where shadow copies are stored), the maximum size should be changed to **No Limit** to reflect the space available on the storage area volume instead of the source volume (where the user files are stored).

Disk space for shadow copies can be allocated on either the same volume as the source files or a different volume. There is a trade-off between ease of use and maintenance versus performance and reliability that the system administrator must consider.

By keeping the shadow copy on the same volume, there is a potential gain in ease of setup and maintenance; however, there may be a reduction in performance and reliability.

△ CAUTION:

If shadow copies are stored on the same volume as the user files, note that a burst of disk input/output (I/O) can cause all shadow copies to be deleted. If the sudden deletion of shadow copies is unacceptable to administrators or end users, it is best to use a separate volume on separate disks to store shadow copies.

Determining creation frequency

The more frequently shadow copies are created, the more likely that end users will get the version that they want. However, with a maximum of 64 shadow copies per volume, there is a trade-off between the frequency of making shadow copies and the amount of time that the earlier files will be available.

By default, the storage system creates shadow copies at 0700 and 1200, Monday through Friday. However, these settings are easily modified by the administrator so that the shadow copy schedule can better accommodate end user needs.

Shadow copies and drive defragmentation

When running Disk Defragmenter on a volume with shadow copies activated, all or some of the shadow copies may be lost, starting with the oldest shadow copies.

If defragmenting volumes on which shadow copies are enabled, use a cluster (or allocation unit) size of 16 KB or larger. Using this allocation unit size reduces the number of copy outs occurring on the snapshot. Otherwise, the number of changes caused by the defragmentation process can cause shadow copies to be deleted faster than expected. Note, however, that NTFS compression is supported only if the cluster size is 4 KB or smaller.

NOTE:

To check the cluster size of a volume, use the `fsutil fsinfo ntfsinfo` command. To change the cluster size on a volume that contains data, back up the data on the volume, reformat it using the new cluster size, and then restore the data.

Mounted drives

A mounted drive is a local volume attached to an empty folder (called a mount point) on an NTFS volume. When enabling shadow copies on a volume that contains mounted drives, the mounted drives are not included when shadow copies are taken. In addition, if a mounted drive is shared and shadow copies are enabled on it, users cannot access the shadow copies if they traverse from the host volume (where the mount point is stored) to the mounted drive.

For example, assume there is a folder `F:\data\users`, and the `Users` folder is a mount point for `G:\`. If shadow copies are enabled on both `F:\` and `G:\`, `F:\data` is shared as `\\server1\data`, and `G:\data\users` is shared as `\\server1\users`. In this example, users can access previous versions of `\\server1\data` and `\\server1\users` but not `\\server1\data\users`.

Managing shadow copies

The vssadmin tool provides a command line capability to create, list, resize, and delete volume shadow copies.

The system administrator can make shadow copies available to end users through a feature called "Shadow Copies for Shared Folders." The administrator uses the Properties menu (see Figure 19) to turn on the Shadow Copies feature, select the volumes to be copied, and determine the frequency with which shadow copies are made.

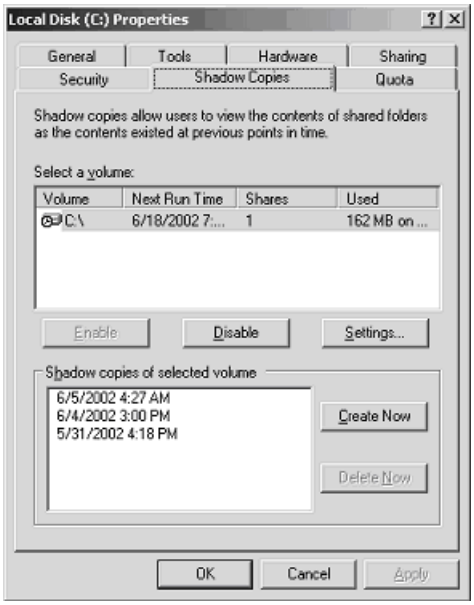


Figure 19 System administrator view of Shadow Copies for Shared Folders

The shadow copy cache file

The default shadow copy settings allocate 10 percent of the source volume being copied (with a minimum of 350 MB), and store the shadow copies on the same volume as the original volume. (See Figure 20). The cache file is located in a hidden protected directory titled "System Volume Information" off of the root of each volume for which shadow copy is enabled.

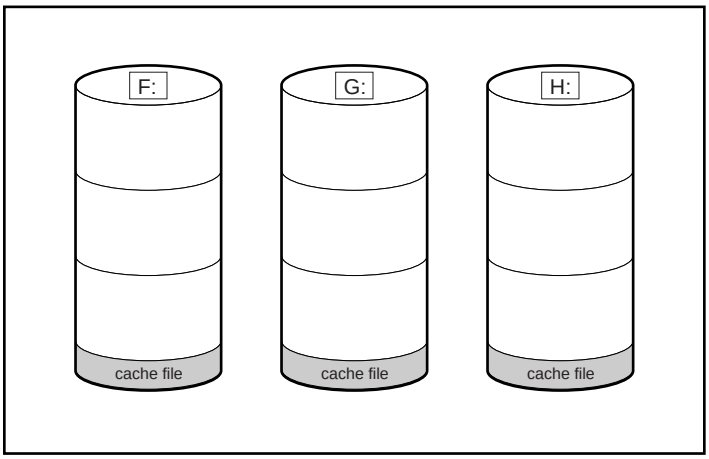


Figure 20 Shadow copies stored on a source volume

The cache file location can be altered to reside on a dedicated volume separate from the volumes containing files shares. (See Figure 21).

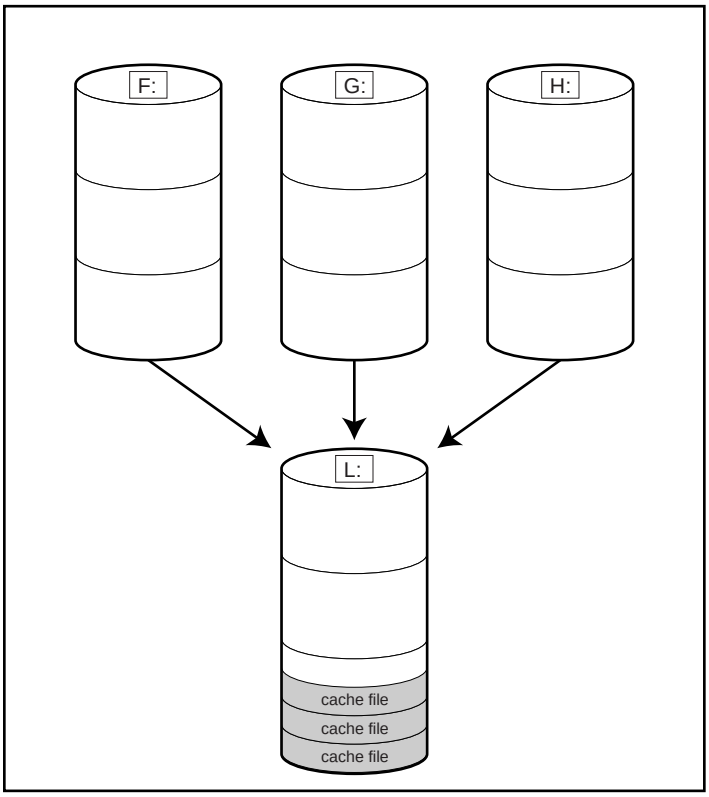


Figure 21 Shadow copies stored on a separate volume

The main advantage to storing shadow copies on a separate volume is ease of management and performance. Shadow copies on a source volume must be continually monitored and can consume space designated for file sharing. Setting the limit too high takes up valuable storage space. Setting the limit too low can cause shadow copies to be purged too soon, or not created at all. By storing shadow copies on a separate volume space, limits can generally be set higher, or set to No Limit. See the online help for instructions on altering the cache file location.

CAUTION:

If the data on the separate volume L: is lost, the shadow copies cannot be recovered.

Enabling and creating shadow copies

Enabling shadow copies on a volume automatically results in several actions:

- Creates a shadow copy of the selected volume.
- Sets the maximum storage space for the shadow copies.
- Schedules shadow copies to be made at 7 a.m. and 12 noon on weekdays.

NOTE:

Creating a shadow copy only makes one copy of the volume; it does not create a schedule.

NOTE:

After the first shadow copy is created, it cannot be relocated. Relocate the cache file by altering the cache file location under Properties prior to enabling shadow copy. See "Viewing shadow copy properties" on page 137.

Viewing a list of shadow copies

To view a list of shadow copies on a volume:

1. Access Disk Management.
2. Select the volume or logical drive, then right-click on it.
3. Select **Properties**.
4. Select **Shadow Copies** tab.

All shadow copies are listed, sorted by the date and time they were created.

NOTE:

It is also possible to create new shadow copies or delete shadow copies from this page.

Set schedules

Shadow copy schedules control how frequently shadow copies of a volume are made. There are a number of factors that can help determine the most effective shadow copy schedule for an organization. These include the work habits and locations of the users. For example, if users do not all live in the same time zone, or they work on different schedules, it is possible to adjust the daily shadow copy schedule to allow for these differences.

Do not schedule shadow copies more frequently than once per hour.

NOTE:

When deleting a shadow copy schedule, that action has no effect on existing shadow copies.

Viewing shadow copy properties

The Shadow Copy Properties page lists the number of copies, the date and time the most recent shadow copy was made, and the maximum size setting.

NOTE:

For volumes where shadow copies do not exist currently, it is possible to change the location of the cache file. Managing the cache files on a separate disk is recommended.

CAUTION:

Use caution when reducing the size limit for all shadow copies. When the size is set to less than the total size currently used for all shadow copies, enough shadow copies are deleted to reduce the total size to the new limit. A shadow copy cannot be recovered after it has been deleted.

Redirecting shadow copies to an alternate volume

IMPORTANT:

Shadow copies must be initially disabled on the volume before redirecting to an alternate volume. If shadow copies are enabled and you disable them, a message appears informing you that all existing shadow copies on the volume will be permanently deleted.

To redirect shadow copies to an alternate volume:

1. Access Disk Management.
2. Select the volume or logical drive, then right-click on it.
3. Select **Properties**.
4. Select the **Shadow Copies** tab.
5. Select the volume that you want to redirect shadow copies from and ensure that shadow copies are disabled on that volume; if enabled, click **Disable**.
6. Click **Settings**.
7. In the **Located on this volume** field, select an available alternate volume from the list.

   NOTE:

   To change the default shadow copy schedule settings, click **Schedule**.

8. Click **OK**.

9. On the **Shadow Copies** tab, ensure that the volume is selected, and then click **Enable**.

Shadow copies are now scheduled to be made on the alternate volume.

Disabling shadow copies

When shadow copies are disabled on a volume, all existing shadow copies on the volume are deleted as well as the schedule for making new shadow copies.

△ CAUTION:

When the Shadow Copies Service is disabled, all shadow copies on the selected volumes are deleted. Once deleted, shadow copies cannot be restored.

Managing shadow copies from the storage system desktop

The storage system desktop can be accessed by using Remote Desktop to manage shadow copies.

To access shadow copies from the storage system desktop:

1. Access the storage system desktop from the primary navigation bar by selecting **Maintenance > Remote Desktop**.
2. Click **My Computer**.
3. Right-click the volume name, and select **Properties**.

4. Click the **Shadow Copies** tab. See Figure 22.

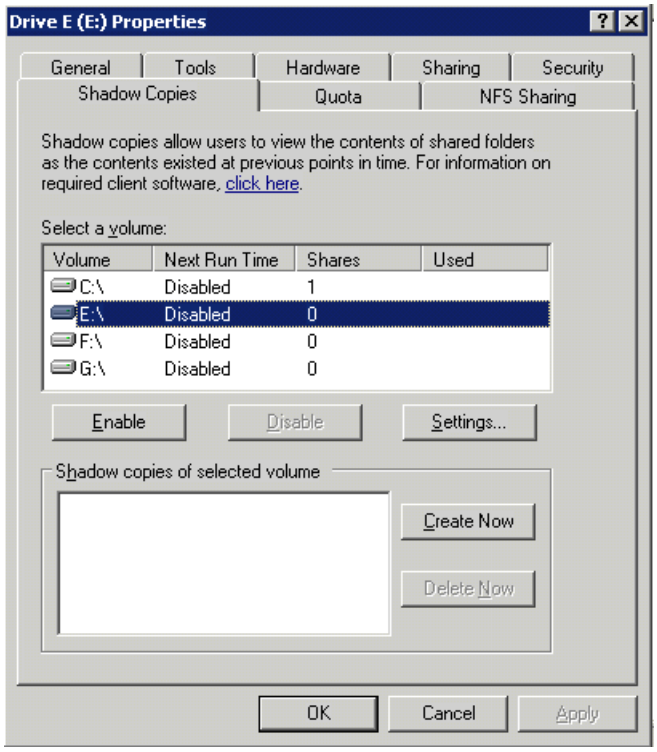


Figure 22 Accessing shadow copies from My Computer

Shadow Copies for Shared Folders

Shadow copies are accessed over the network by supported clients and protocols. There are two sets of supported protocols, SMB and NFS. All other protocols are not supported; this would include HTTP, FTP, AppleTalk, and NetWare Shares. For SMB support, a client-side application denoted as Shadow Copies for Shared Folders is required. The client-side application is currently only available for Windows XP and Windows 2000 SP3+.

No additional software is required to enable UNIX users to independently retrieve previous versions of files stored on NFS shares.

NOTE:

Shadow Copies for Shared Folders supports retrieval only of shadow copies of network shares. It does not support retrieval of shadow copies of local folders.

NOTE:

Shadow Copies for Shared Folders clients are not available for HTTP, FTP, AppleTalk, or NetWare shares. Consequently, users of these protocols cannot use Shadow Copies for Shared Folders to independently retrieve previous versions of their files. However, administrators can take advantage of Shadow Copies for Shared Folders to restore files for these users.

SMB shadow copies

Windows users can independently access previous versions of files stored on SMB shares by using the Shadow Copies for Shared Folders client. After the Shadow Copies for Shared Folders client is installed on the user's computer, the user can access shadow copies for a share by right-clicking on the share to open its Properties window, clicking the **Previous Versions** tab, and then selecting the desired shadow copy. Users can view, copy, and restore all available shadow copies.

Shadow Copies for Shared Folders preserves the permissions set in the access control list (ACL) of the original folders and files. Consequently, users can only access shadow copies for shares to which they have access. In other words, if a user does not have access to a share, he also does not have access to the share's shadow copies.

The Shadow Copies for Shared Folders client pack installs a **Previous Versions** tab in the **Properties** window of files and folders on network shares.

Users access shadow copies with Windows Explorer by selecting **View**, **Copy**, or **Restore** from the **Previous Versions** tab. (See Figure 23). Both individual files and folders can be restored.

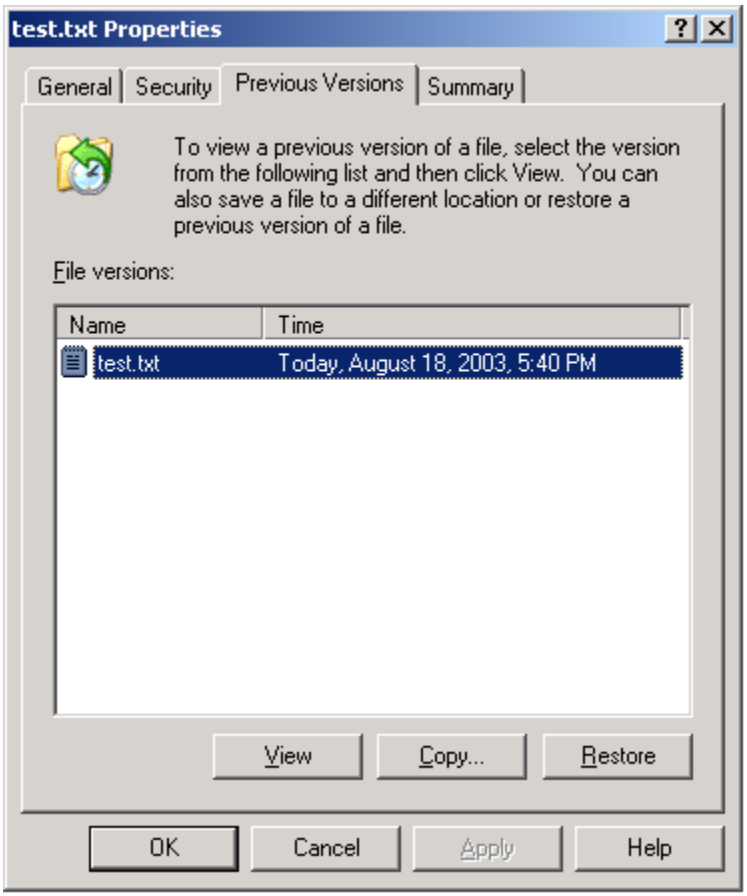


Figure 23 Client GUI

When users view a network folder hosted on the storage system for which shadow copies are enabled, old versions (prior to the snapshot) of a file or directory are available. Viewing the properties of the file or folder presents users with the folder or file history—a list of read-only, point-in-time copies of the file or folder contents that users can then open and explore like any other file or folder. Users can view files in the folder history, copy files from the folder history, and so on.

NFS shadow copies

UNIX users can independently access previous versions of files stored on NFS shares via the NFS client; no additional software is required. Server for NFS exposes each of a share's available shadow copies as a pseudo-subdirectory of the share. Each of these pseudo-subdirectories is displayed in exactly the same way as a regular subdirectory is displayed.

The name of each pseudo-subdirectory reflects the creation time of the shadow copy, using the format .@GMT-YYYY.MM.DD-HH:MM:SS. To prevent common tools from needlessly enumerating the pseudo-subdirectories, the name of each pseudo-subdirectory begins with the dot character, thus rendering it hidden.

The following example shows an NFS share named “NFSShare” with three shadow copies, taken on April 27, 28, and 29 of 2003 at 4 a.m.

NFSShare

.@GMT-2003.04.27-04:00:00

.@GMT-2003.04.28-04:00:00

.@GMT-2003.04.29-04:00:00

Access to NFS shadow copy pseudo-subdirectories is governed by normal access-control mechanisms using the permissions stored in the file system. Users can access only those shadow copies to which they have read access at the time the shadow copy is taken. To prevent users from modifying shadow copies, all pseudo-subdirectories are marked read-only, regardless of the user's ownership or access rights, or the permissions set on the original files.

Server for NFS periodically polls the system for the arrival or removal of shadow copies and updates the root directory view accordingly. Clients then capture the updated view the next time they issue a directory read on the root of the share.

Recovery of files or folders

There are three common situations that may require recovery of files or folders:

- Accidental file deletion, the most common situation
- Accidental file replacement, which may occur if a user selects Save instead of Save As
- File corruption

It is possible to recover from all of these scenarios by accessing shadow copies. There are separate steps for accessing a file compared to accessing a folder.

Recovering a deleted file or folder

To recover a deleted file or folder within a folder:

1. Access to the folder where the deleted file was stored.
2. Position the cursor over a blank space in the folder. If the cursor hovers over a file, that file is selected.
3. Right-click, select **Properties** from the bottom of the menu, and then click the **Previous Versions** tab.
4. Select the version of the folder that contains the file before it was deleted, and then click **View**.
5. View the folder and select the file or folder to recover. The view may be navigated multiple folders deep.

6. Click **Restore** to restore the file or folder to its original location. Click **Copy...** to allow the placement of the file or folder to a new location.

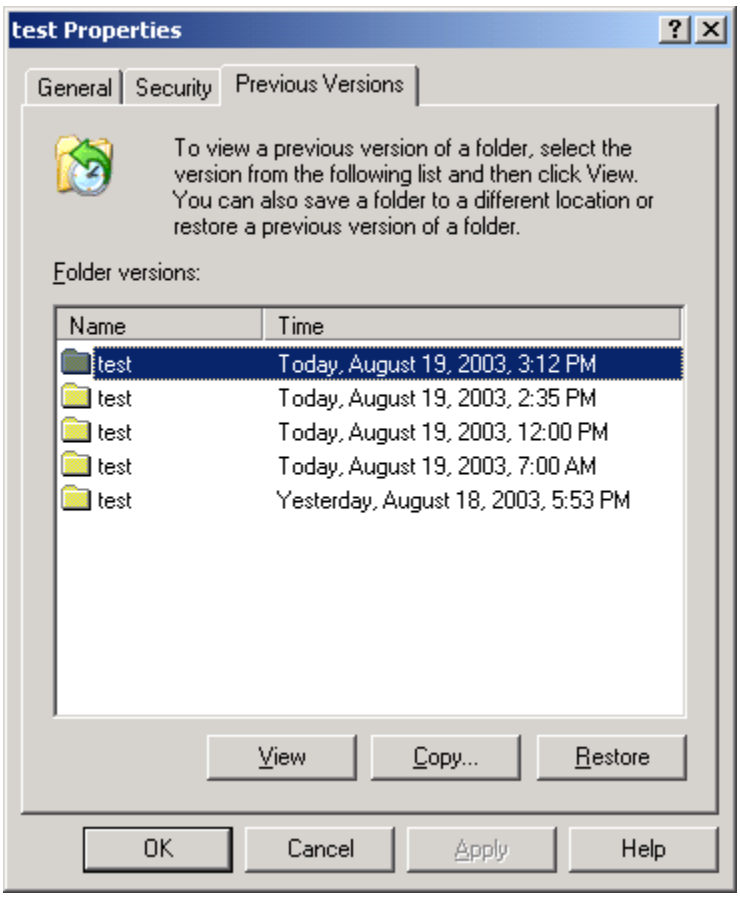


Figure 24 Recovering a deleted file or folder

Recovering an overwritten or corrupted file

Recovering an overwritten or corrupted file is easier than recovering a deleted file because the file itself can be right-clicked instead of the folder. To recover an overwritten or corrupted file:

1. Right-click the overwritten or corrupted file, and then click **Properties**.
2. Click **Previous Versions**.
3. To view the old version, click **View**. To copy the old version to another location, click **Copy...** to replace the current version with the older version, click **Restore**.

Recovering a folder

To recover a folder:

1. Position the cursor so that it is over a blank space in the folder to be recovered. If the cursor hovers over a file, that file is selected.
2. Right-click, select **Properties** from the bottom of the menu, and then click the **Previous Versions** tab.

3. Click either **Copy...** or **Restore**.

   Clicking **Restore** enables the user to recover everything in that folder as well as all subfolders. Clicking **Restore** does not delete any files.

Backup and shadow copies

Shadow copies are only available on the network via the client application, and only at a file or folder level as opposed to the entire volume. Hence, the standard backup associated with a volume backup will not work to back up the previous versions of the file system. To answer this particular issue, shadow copies are available for back up in two situations. If the backup software in question supports the use of shadow copies and can communicate with underlying block device, it is supported, and the previous version of the file system will be listed in the backup application as a complete file system snapshot. If the built-in backup application NTbackup is used, the backup software forces a snapshot, and then uses the snapshot as the means for back up. The user is unaware of this activity and it is not self-evident although it does address the issue of open files.

Shadow Copy Transport

Shadow Copy Transport provides the ability to transport data on a Storage Area Network (SAN). With a storage array and a VSS-aware hardware provider, it is possible to create a shadow copy on one server and import it on another server. This process, essentially "virtual" transport, is accomplished in a matter of minutes, regardless of the size of the data.

NOTE:

Shadow copy transport is supported only on Windows Server 2003 Enterprise Edition, Windows Storage Server 2003 Enterprise Edition, and Windows Server 2003 Datacenter Edition. It is an advanced solution that works only if it has a hardware provider on the storage array.

A shadow copy transport can be used for a number of purposes, including:

- Tape backups

  An alternative to traditional backup to tape processes is transport of shadow copies from the production server onto a backup server, where they can then be backed up to tape. Like the other two alternatives, this option removes backup traffic from the production server. While some backup applications might be designed with the hardware provider software that enables transport, others are not. The administrator should determine whether or not this functionality is included in the backup application.

- Data mining

  The data in use by a particular production server is often useful to different groups or departments within an organization. Rather than add additional traffic to the production server, a shadow copy of the data can be made available through transport to another server. The shadow copy can then be processed for different purposes, without any performance impact on the original server.

The transport process is accomplished through a series of DISKRAID command steps:

1. Create a shadow copy of the source data on the source server (read-only).
2. Mask off (hide) the shadow copy from the source server.
3. Unmask the shadow copy to a target server.
4. Optionally, clear the read-only flags on the shadow copy.

The data is now ready to use.

Folder and share management

The HP All-in-One Storage System supports several file-sharing protocols, including DFS, NFS, FTP, HTTP, and Microsoft SMB. This section discusses overview information as well as procedures for the setup and management of the file shares for the supported protocols. Security at the file level and at the share level is also discussed.

NOTE:

Detailed information on setting up and managing NFS and NCP shares is discussed in Microsoft Services for Network File System (MSNFS).

Folder management

Volumes and folders on any system are used to organize data. Regardless of system size, systematic structuring and naming conventions of volumes and folders eases the administrative burden. Moving from volumes to folders to shares increases the level of granularity of the types of data stored in the unit and the level of security access allowed.

Folders can be managed using the HP All-in-One Management Console. Tasks include:

- Accessing a specific volume or folder
- Creating a new folder
- Deleting a folder
- Modifying folder properties
- Creating a new share for a volume or folder
- Managing shares for a volume or folder

Managing file-level permissions

Security at the file level is managed using Windows Explorer.

File level security includes settings for permissions, ownership, and auditing for individual files.

To enter file permissions:

1. Using Windows Explorer, access the folder or file that needs to be changed, and then right-click the folder.

2. Click **Properties**, and then click the **Security** tab.

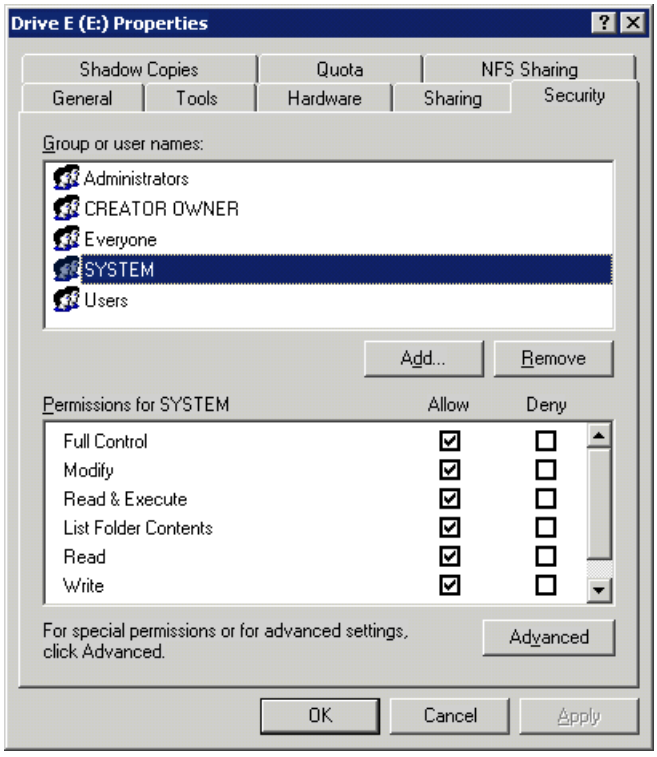


Figure 25 Properties dialog box, Security tab

Several options are available on the **Security** tab:

- To add users and groups to the permissions list, click **Add**. Follow the dialog box instructions.
- To remove users and groups from the permissions list, highlight the desired user or group, and then click **Remove**.
- The center section of the **Security** tab lists permission levels. When new users or groups are added to the permissions list, select the appropriate boxes to configure the common file-access levels.

3. To modify ownership of files, or to modify individual file access level permissions, click **Advanced**.

   Figure 26 illustrates the properties available on the **Advanced Security Settings** dialog box.

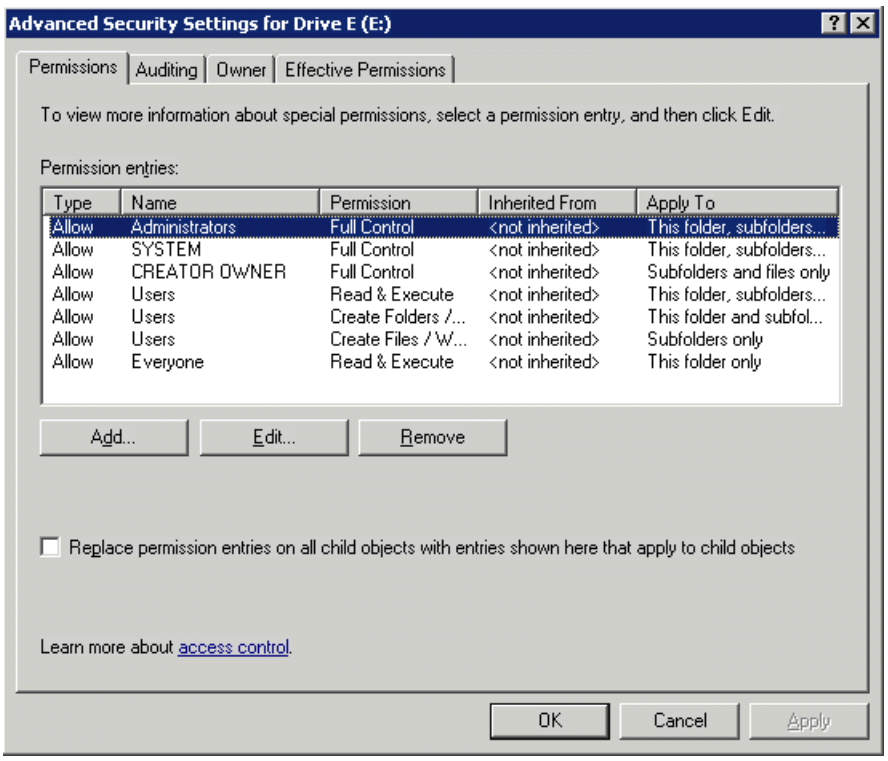


Figure 26 Advanced Security settings dialog box, Permissions tab

Other functionality available in the **Advanced Security Settings** dialog box is illustrated in Figure 26 and includes:

- Add a new user or group—Click **Add**, and then follow the dialog box instructions.
- Remove a user or group— Click **Remove**.
- Replace permission entries on all child objects with entries shown here that apply to child objects—This allows all child folders and files to inherit the current folder permissions by default.
- Modify specific permissions assigned to a particular user or group—Select the desired user or group, and then click **Edit**.

4. Enable or disable permissions by selecting the **Allow** box to enable permission or the **Deny** box to disable permission. If neither box is selected, permission is automatically disabled. Figure 27 illustrates the **Edit** screen and some of the permissions.

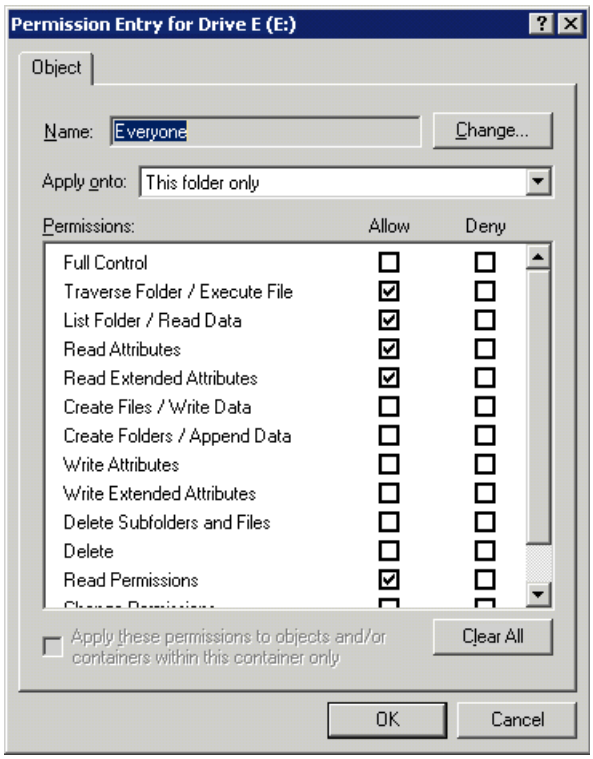


Figure 27 User or group Permission Entry dialog box

Another area of the **Advanced Security Settings** is the **Auditing** tab. Auditing allows you to set rules for the auditing of access, or attempted access, to files or folders. Users or groups can be added, deleted, viewed, or modified through the **Advanced Security Settings Auditing** tab.

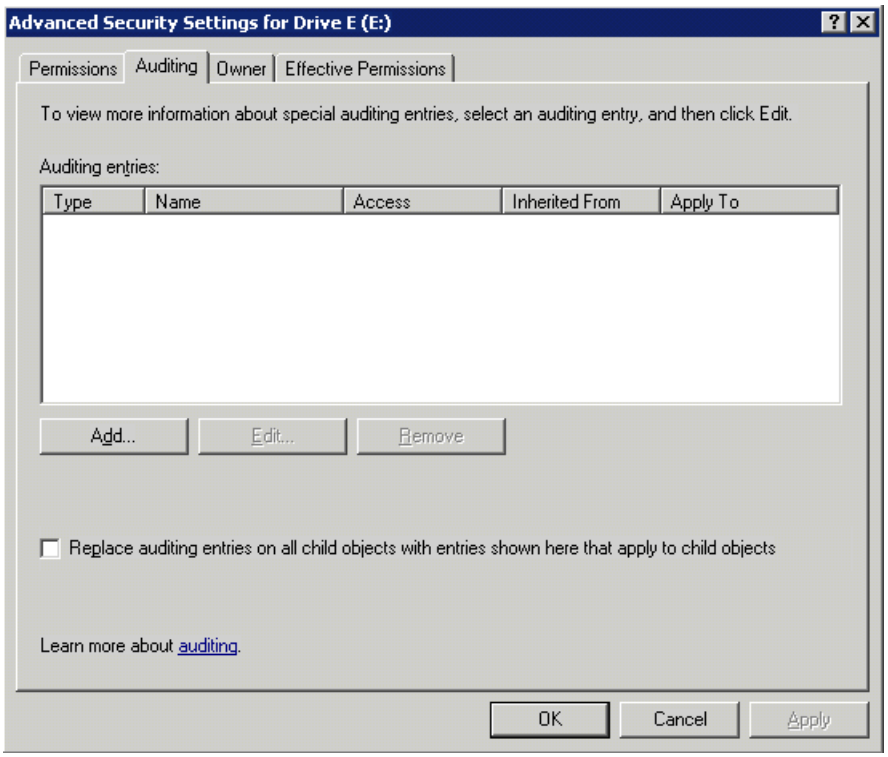


Figure 28 Advanced Security Settings dialog box, Auditing tab

5. Click **Add** to display the Select User or Group dialog box.

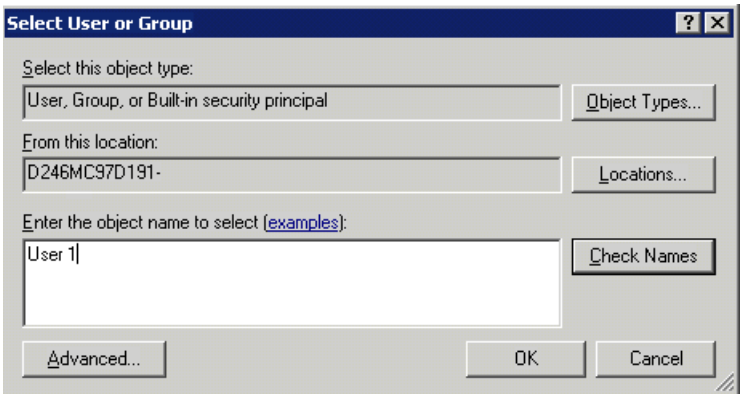


Figure 29 Select User or Group dialog box

NOTE:

Click Advanced to search for users or groups.

6. Select the user or group.

7. Click **OK**.

   The **Auditing Entry** dialog box is displayed.

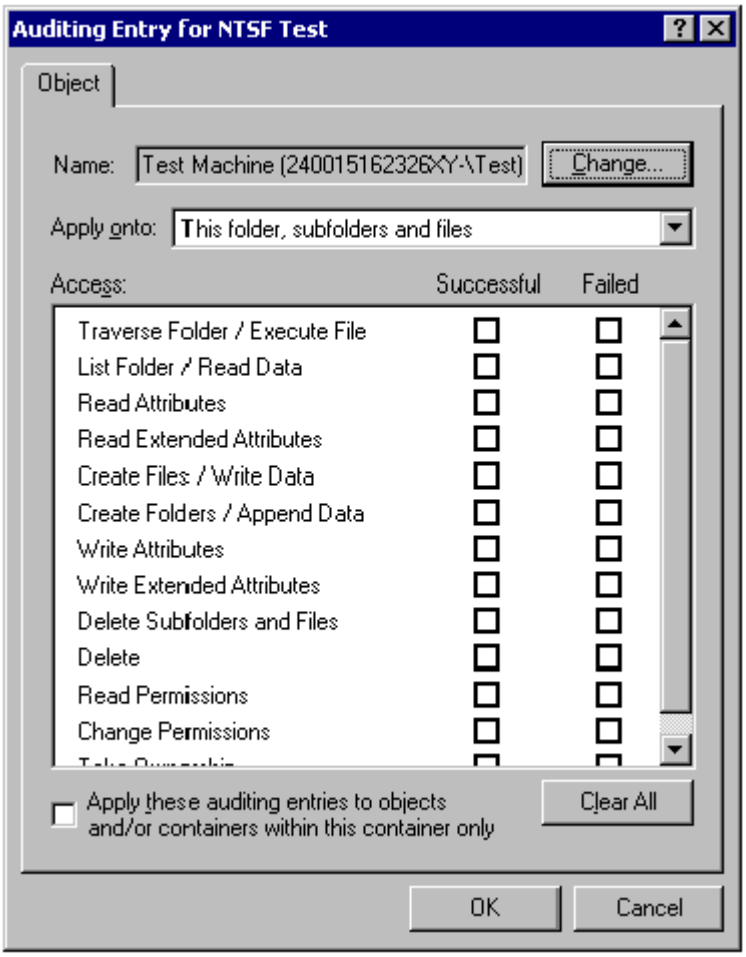


Figure 30 Auditing Entry dialog box for folder name NTFS Test

8. Select the desired **Successful** and **Failed** audits for the user or group.
9. Click **OK**.

NOTE:

Auditing must be enabled to configure this information. Use the local Computer Policy Editor to configure the audit policy on the storage system.

The **Owner** tab allows taking ownership of files. Typically, administrators use this area to take ownership of files when the file ACL is incomplete or corrupt. By taking ownership, you gain access to the files, and then manually apply the appropriate security configurations.

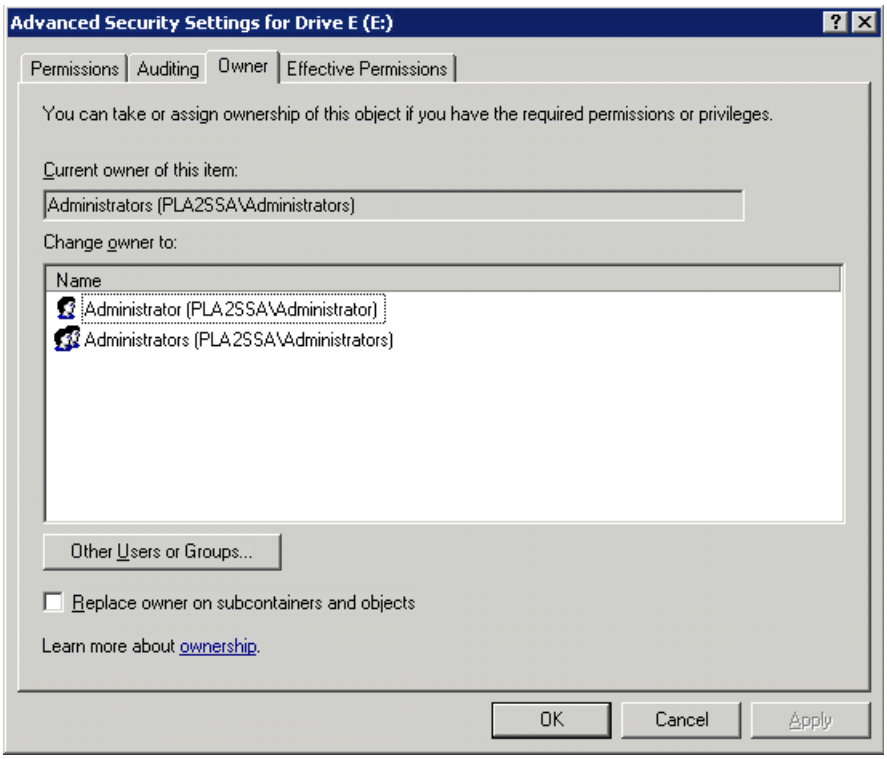


Figure 31 Advanced Security Settings dialog box, Owner tab

The current owner of the file or folder is listed at the top of the screen. To take ownership:

1. Click the appropriate user or group in the **Change owner to** list.
2. If it is also necessary to take ownership of subfolders and files, enable the **Replace owner on subcontainers and objects** box.
3. Click **OK**.

Share management

There are several ways to set up and manage shares. Methods include using Windows Explorer, a command line interface, or the HP All-in-One Management Console.

As previously mentioned, the file-sharing security model of the storage system is based on the NTFS file-level security model. Share security seamlessly integrates with file security. In addition to discussing share management, this section discusses share security.

Share considerations

Planning the content, size, and distribution of shares on the storage system can improve performance, manageability, and ease of use.

The content of shares should be carefully chosen to avoid two common pitfalls: either having too many shares of a very specific nature, or of having very few shares of a generic nature. For example, shares for general use are easier to set up in the beginning, but can cause problems later. Frequently, a better approach is to create separate shares with a specific purpose or group of users in mind. However, creating too many shares also has its drawbacks. For example, if it is sufficient to create a single share for user home directories, create a “homes” share rather than creating separate shares for each user.

By keeping the number of shares and other resources low, the performance of the storage system is optimized. For example, instead of sharing out each individual user's home directory as its own share, share out the top-level directory and let the users map personal drives to their own subdirectory.

Defining Access Control Lists

The Access Control List (ACL) contains the information that dictates which users and groups have access to a share, as well as the type of access that is permitted. Each share on an NTFS file system has one ACL with multiple associated user permissions. For example, an ACL can define that User1 has read and write access to a share, User2 has read only access, and User3 has no access to the share. The ACL also includes group access information that applies to every user in a configured group. ACLs are also referred to as permissions.

Integrating local file system security into Windows domain environments

ACLs include properties specific to users and groups from a particular workgroup server or domain environment. In a multidomain environment, user and group permissions from several domains can apply to files stored on the same device. Users and groups local to the storage system can be given access permissions to shares managed by the device. The domain name of the storage system supplies the context in which the user or group is understood. Permission configuration depends on the network and domain infrastructure where the server resides.

File-sharing protocols (except NFS) supply a user and group context for all connections over the network. (NFS supplies a machine-based context.) When new files are created by those users or machines, the appropriate ACLs are applied.

Configuration tools provide the ability to share permissions out to clients. These shared permissions are propagated into a file system ACL, and when new files are created over the network, the user creating the file becomes the file owner. In cases where a specific subdirectory of a share has different permissions from the share itself, the NTFS permissions on the subdirectory apply instead. This method results in a hierarchical security model where the network protocol permissions and the file permissions work together to provide appropriate security for shares on the device.

NOTE:

Share permissions and file-level permissions are implemented separately. It is possible for files on a file system to have different permissions from those applied to a share. When this situation occurs, the file-level permissions override the share permissions.

Comparing administrative (hidden) and standard shares

CIFS supports both administrative shares and standard shares.

- Administrative shares are shares with a last character of $. Administrative shares are not included in the list of shares when a client browses for available shares on a CIFS server.
- Standard shares are shares that do not end in a $ character. Standard shares are listed whenever a CIFS client browses for available shares on a CIFS server.

The storage system supports both administrative and standard CIFS shares. To create an administrative share, end the share name with the $ character when setting up the share. Do not type a $ character at the end of the share name when creating a standard share.

Managing shares

Shares can be managed using the HP All-in-One Management Console. Tasks include:

- Creating a new share
- Deleting a share
- Modifying share properties
- Publishing in DFS

△ CAUTION:

Before deleting a share, warn all users to exit that share and confirm that no one is using that share.

File Server Resource Manager

File Server Resource Manager (FSRM) is a suite of tools that allows administrators to understand, control, and manage the quantity and type of data stored on their servers. Some of the tasks you can perform are:

- Quota management
- File screening management
- Storage reports

The HP All-in-One Management Console provides access to FSRM tasks.

For procedures and methods beyond what are described below, see the online help. In addition, see a Microsoft File Server Resource Manager white paper available at http://download.microsoft.com/download/7/4/7/7472bf9b-3023-48b7-87be-d2cedc38f15a/WS03R2_Storage_Management.doc .

Quota management

On the Quota Management node of the File Server Resource Manager snap-in, you can perform the following tasks:

- Create quotas to limit the space allowed for a volume or folder and generate notifications when the quota limits are approached or exceeded.
- Generate auto quotas that apply to all existing folders in a volume or folder, as well as to any new subfolders created in the future.
- Define quota templates that can be easily applied to new volumes or folders and that can be used across an organization.

File screening management

On the File Screening Management node of the File Server Resource Manager snap-in, you can perform the following tasks:

- Create file screens to control the types of files that users can save and to send notifications when users attempt to save blocked files.
- Define file screening templates that can be easily applied to new volumes or folders and that can be used across an organization.
- Create file screening exceptions that extend the flexibility of the file screening rules.

Storage reports

On the Storage Reports node of the File Server Resource Manager snap-in, you can perform the following tasks:

- Schedule periodic storage reports that allow you to identify trends in disk usage.
- Monitor attempts to save unauthorized files for all users or a selected group of users.
- Generate storage reports instantly.

Other Windows disk and data management tools

When you install certain tools, such as Windows Support Tools or Windows Resource Kit Tools, information about these tools might appear in Help and Support Center. To see the tools that are available to you, look in the Help and Support Center under **Support Tasks**, click **Tools**, and then click **Tools by Category**.

NOTE:

The Windows Support Tools and Windows Resource Kit Tools, including documentation for these tools, are available in English only. If you install them on a non-English language operating system or on an operating system with a Multilingual User Interface Pack (MUI), you see English content mixed with non-English content in Help and Support Center. To see the tools that are available to you, click **Start**, click **Help and Support Center**, and then, under **Support Tasks**, click **Tools**.

Additional information and references for file services

Backup

HP recommends that you back up the print server configuration whenever a new printer is added to the network and the print server configuration is modified. For details on implementing the backup solution, see the *Medium Business Guide for Backup and Recovery*. The guide can be viewed or downloaded from Microsoft at http://www.microsoft.com/technet/itsolutions/smbiz/mits/br/mit_br.mspx.

HP StorageWorks Library and Tape Tools

HP StorageWorks Library and Tape Tools (L&TT) provides functionality for firmware downloads, verification of device operation, maintenance procedures, failure analysis, corrective service actions, and some utility functions. It also provides seamless integration with HP hardware support by generating and e-mailing support tickets that deliver a snapshot of the storage system.

For more information, and to download the utility, see the StorageWorks L&TT website at http://h18006.www1.hp.com/products/storageworks/ltt.

Antivirus

The server should be secured by installing the appropriate antivirus software. For details on implementing antivirus, see the Medium Business Guide for Antivirus. The guide can be viewed or

downloaded from Microsoft at http://www.microsoft.com/technet/itsolutions/smbiz/mits/av/mit_av.mspx.

Security

For guidance on hardening file servers, see the *Microsoft Windows Server 2003 Security Guide*. The guide can be viewed or downloaded at http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx.

More information

The following web sites provide detailed information for using print services with Windows Server 2003, which also applies to Windows Storage Server 2003.

- Microsoft Storage
  http://www.microsoft.com/windowsserversystem/storage/default.mspx
- Microsoft Windows Storage Server 2003
  http://www.microsoft.com/windowsserversystem/wss2003/default.mspx
- Performance Tuning Guidelines for Windows Server 2003
  http://www.microsoft.com/windowsserver2003/evaluation/performance/tuning.mspx
- Windows SharePoint Services
  http://www.microsoft.com/windowsserver2003/technologies/sharepoint/default.mspx

B Print services

Microsoft Print Management Console

Print Management in the Microsoft Windows Server 2003 R2 operating system is a Microsoft Management Console (MMC) snap-on that system administrators can use to perform common print management tasks in a large enterprise. It provides a single interface that administrators can use to perform printer and print server management tasks efficiently with detailed control. You can use Print Management from any computer running Windows Server 2003 R2, and you can manage all network printers on print servers running Windows 2000 Server, Windows Server 2003, or Windows Server 2003 R2.

New or improved HP print server features

HP Web Jetadmin

WJA is a web-based tool for remotely installing, configuring, and managing a wide variety of HP and non-HP network peripherals using only a web browser. It supports a modular design, whereby plug-ins can be installed to provide additional device, language, and application functionality. WJA is not preinstalled on the storage system, but can be installed (see "HP Web Jetadmin installation" on page 156).

HP Install Network Printer Wizard

The inclusion of the HP Install Network Printer Wizard (INPW) utility on the factory image is new. INPW simplifies the process of installing network printers, including configuration settings on the print server. INPW identifies HP Jetdirect network print devices and allows the user to select the printer to install on the print server.

HP Download Manager for Jetdirect Print Devices

The inclusion of the HP Download Manager (DLM) for Jetdirect Printer Devices on the factory image is new. DLM is used to upgrade HP Jetdirect print server firmware on HP network printers. The utility obtains the latest firmware catalog from either from the Internet or from a computer with the download firmware images already in place. The DLM discovers all or user-selected Jetdirect devices and upgrades those based on the firmware catalog.

Microsoft Print Migrator Utility

The inclusion of the Microsoft Print Migrator utility on the factory image is new. The utility provides complete printer configuration backup of the print server to a user-specified CAB file. Print Migrator supports migration of print configuration data between different versions of Windows, and supports conversion of line printer remote (LPR) ports to the Standard TCP/IP Port Monitor on Windows 2000, Windows XP, and Windows Server 2003.

Network printer drivers

Updated print drivers for HP network printers are preinstalled on the storage system. If a Service Release DVD has been run on the server, there are updated HP network print drivers in the `C:\hpnas\PRINTERS` folder.

Print services management

Print services information to plan, set up, manage, administer, and troubleshoot print servers and print devices are available online using the Help and Support Center feature. To access the Help and Support Center, select **Start > Help and Support**, then **Printers and Faxes** under Help Contents.

Microsoft Print Management Console

The Print Management Console (PMC) can be started from the HP All–in-One Management Console, or the PMC snap-in can be added to the Microsoft Management Console.

HP recommends that you use the *Microsoft Print Management Step-by-Step Guide* on the Documentation CD for print concepts, use of the PMC, and management of network printers. The guide can also be downloaded from http://www.microsoft.com/printserver.

When running the PMC on a server that has Windows Firewall enabled, no printers will be displayed in the printers folder of the PMC. In order for printers to be displayed, you need to open the file and print sharing ports (TCP 139 and 445, and UDP 137 and 138). If this does not fix the problem, or if these ports are already open, you may need to turn off the Windows Firewall to display printers.

To open the file and print sharing ports:

1. Click **Start**, point to Control Panel, and click **Windows Firewall**.
2. On the Exceptions tab, ensure that the File and Printer Sharing check box is selected and click **OK**.

To turn off Windows Firewall:

1. Click **Start**, point to Control Panel, and click **Windows Firewall**.
2. Select **Off** (not recommended) and click **OK**.

HP Web Jetadmin installation

HP Web Jetadmin is used to manage a fleet of HP and non-HP network printers and other peripherals using a web browser. Although not preinstalled, the Web Jetadmin software is located in the `C:\hpnas\Components\WebJetadmin` folder, and can be installed by running the `WJA.exe` setup program. Follow the installation wizard and supply a password for the local "Admin" username account and a system name.

For more information about Web Jetadmin and Web Jetadmin plug-ins, see http://www.hp.com/go/webjetadmin. For an article on optimizing performance, see http://h10010.www1.hp.com/wwpc/pscmisc/vac/us/product_pdfs/weboptim.pdf.

Web-based printer management and Internet printing

Internet printing is enabled by default on the print server. Internet printing consists of two main components:

- Web-based printer management with the ability to administer, connect to, and view printers through a web browser.
- Internet printing enabling users to connect to a printer using the printer's URL.

A Microsoft white paper discussing the uses of both components can be obtained at http://www.microsoft.com/windowsserver2003/techinfo/overview/internetprint.mspx.

Planning considerations for print services

Before configuring the print server, the following checklist of items should be followed:

1. **Determine the operating system version of the clients that will send jobs to this printer**. This information is used to select the correct client printer drivers for the client and server computers using the printer. Enabling this role on the print server allows the automatic distribution of these drivers to the clients. Additionally, the set of client operating systems determines which of these drivers need to be installed on the server during the print server role installation.
2. **At the printer, print a configuration or test page that includes manufacturer, model, language, and installed options**. This information is needed to choose the correct printer driver. The manufacturer and model are usually enough to uniquely identify the printer and its language. However, some printers support multiple languages, and the configuration printout usually lists them. Also, the configuration printout often lists installed options, such as extra memory, paper trays, envelope feeders, and duplex units.
3. **Choose a printer name**. Users running Windows-based client computers choose a printer by using the printer name. The wizard that you will use to configure your print server provides a default name, consisting of the printer manufacturer and model. The printer name is usually fewer than 31 characters in length.
4. **Choose a share name**. A user can connect to a shared printer by entering this name, or by selecting it from a list of share names. The share name is usually fewer than 8 characters for compatibility with MS-DOS and Windows 3.x clients.
5. (Optional) **Choose a location description and a comment**. These can help identify the location of the printer and provide additional information. For example, the location could be “Second floor, copy room” and the comment could be “Additional toner cartridges are available in the supply room on floor 1."
6. **Enable management features for Active Directory and Workgroup Environments**. If the print server is part of an Active Directory domain rather than Workgroup, the print server enables the following management features:
   - Restrict access to printer-based domain user accounts.
   - Publish shared printers to Active Directory to aid in search for the resource.
7. **Deploy printers using group policy**. Print management can be used with Group Policy to automatically add printer connections to a server's Printers and Faxes folder. For more information, see the Microsoft article at http://technet2.microsoft.com/WindowsServer/en/Library/ab8d75f8-9b35-4e3e-a344-90d7799927231033.mspx.
8. **Determine whether printer spooling be enabled**. Two or more identical printers that are connected to one print server can act as a single printer. As a means to load-balance print queues when you print a document, the print job is sent to the first available printer in the pool. See “Setting Printer Properties” in the Windows online help for additional information.

Print queue creation

In addition to Windows Printer and Faxes, Add Printer Wizard, the HP Install Network Printer Wizard (INPW) utility discovers HP Jetdirect network printers on the local network and allows print queues to

be created on the print server. The utility is located on the storage system in the `C:\hpnas\Components\Install Network Printer Wizard` folder.

Sustaining print administration tasks

Tasks that need to be performed regularly to support the print services include:

- Monitoring print server performance using the built-in performance monitoring tool in the Windows Server operating system.
- Supporting printers that include adding, moving, and removing printers as requirements change.
- Installing new printer drivers.
- Recording information about the printer's name, share names, printer features, and the location where the printers are physically installed. This information should be kept in an easily accessible place.

For process suggestions for recurring tasks, see the Microsoft Print Service Product Operations Guide at http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/pspog/pspog3/mspx.

Driver updates

Print drivers

The latest print drivers for many HP network printers are supplied on the Service Release DVD. If selected as part of the service release installation process, updated print drivers are copied to the print drivers folder `C:\hpnas\PRINTERS` on the storage system. Print drivers are also available for download on the HP Support web site for individual network printers.

User-mode vs. kernel-mode drivers

Drivers can be written in either user mode (also called version 3 drivers) or kernel mode (also called version 2 drivers). Native drivers on Windows 2000 and later run in user mode. Windows Server 2003 and Windows Storage Server 2003 can run kernel-mode drivers, although this is not recommended for stability reasons.

Kernel-mode driver installation blocked by default

In Windows Server 2003 and Windows Storage Server 2003, installation of kernel-mode drivers is blocked by default.

To allow kernal-mode drivers to be installed, perform the following steps:

1. Open Group Policy, click **Start > Run**, then type **gpedit.msc**, and press **Enter**.
2. Under **Local Computer Policy**, double-click **Computer Configuration**.
3. Right-click **Disallow installation of printers using kernel-mode drivers** and then click **Properties**.
4. On the **Setting** tab, click either **Not Configured** or **Disabled**, and then click **OK**.

HP Jetdirect firmware

The HP Download Manager (DLM) utility for Jetdirect printers provides upgrades of HP Jetdirect print server firmware on HP network printers. The utility is located on the storage system in the `C:\hpnas\Components\Download Manager for Jetdirect` folder. A connection to the

Internet is required, or the utility can be pointed to a local location where the firmware images are stored. For more information on upgrading HP Jetdirect print server firmware, see http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj06917.

Printer server scalability and sizing

A Microsoft technical paper overviews several key factors that influence the capacity of a given print server configuration. While this paper cannot provide a predictive formula to determine the printing throughput of a given configuration, it does describe several reference systems and their capacity. This paper also presents the information necessary to help the system administrator or capacity planner estimate, and later monitor, their server workload. The current version of this paper is maintained at http://www.microsoft.com/printserver.

Backup

It is recommended that you back up the print server configuration whenever a new printer is added to the network and the print server configuration is modified. For details on implementing the backup solution, refer to the *Medium Business Guide for Backup and Recovery*. The guide can be viewed or downloaded from Microsoft at http://www.microsoft.com/technet/itsolutions/smbiz/mits/br/mit_br.mspx.

The Print Migrator utility is recommended as a print-specific alternative to backing up print configuration settings on the print server. The Print Migrator utility is located in the `C:\hpnas\Components\PrintMigrator` folder on the storage system.

For more information about the Print Migrator utility, see http://www.microsoft.com/WindowsServer2003/techinfo/overview/printmigrator3.1.mspx.

Best practices

The following is practical advice for managing print devices:

- Printers and print servers should be published in Active Directory.
- Locate printers in common areas, such as near conference rooms.
- Protect print servers using antivirus software.
- Ensure the print server is included in the backup configuration.
- Use Microsoft Printer Migrator to back up a print server configuration and restore settings on a new print server. This eliminates the need to manually re-create print queues and printer ports, install drivers, and change the IP configuration.
- Use Microsoft Printer Migrator to backup new printers configured on the print server.
- Use Microsoft Printer Migrator when migrating to new print servers.
- Perform a full backup of the print server, including the state information, before releasing the system to the users in the production environment.
- Whenever a new configuration is made or existing configuration is modified, a backup should be performed.
- To optimize performance, move the print spooler to another disk, separate from the disk supporting the operating system. To move the print spooler to another disk:
  - Start Printer and Faxes.
  - On the File menu, click **Server Properties**, and then click the **Advanced** tab.
  - In the Spool folder window, enter the path and the name of the new default spool folder for the print server, and then click **Apply** or **OK**.

- Stop and restart the spooler service, or restart the print server.

Troubleshooting

The online help or Help and Support Center feature should be used to troubleshoot general and common print-related problems. Printing help can be accessed by selecting **Start > Help and Support**, then the **Printers and Faxes** selection under **Help Contents**.

The same print troubleshooting information can be accessed at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/2048a7ba-ec57-429c-95a3-226eea32d126.mspx

Specific print server related problems as well as other system related known issues and workarounds are addressed in release notes. To view the latest version, see http://www.hp.com/go/support. Select **See support and troubleshooting information** and enter a product name/number. Under **self-help resources**, select the **manuals (guides, supplements, addendums, etc)** link.

Additional references for print services

The following Web sites provide detailed information for using print services with Windows Server 2003, which also applies to Windows Storage Server 2003.

- Windows Server 2003 print services home page at http://www.microsoft.com/windowsserver2003/technologies/print/default.mspx
- Medium Business Solution for Print Services at http://www.microsoft.com/technet/itsolutions/smbiz/mits/ps/mit_ps.mspx.

C Microsoft Services for Network File System (MSNFS)

This chapter discusses networking features in Microsoft Services for Network File System (MSNFS).

MSNFS Features

MSNFS is an update to the NFS components that were previously available in Services for UNIX 3.5.

MSNFS includes the following new features:

- Updated administration snap-in—MSNFS Administration
- Active Directory Lookup—The Identity Management for UNIX Active Directory schema extension, available in Microsoft Windows Server 2003 R2, includes UNIX user identifier (UID) and group identifier (GID) fields, which enables Server for NFS and Client for NFS to look up Windows-to-UNIX user account mappings directly from Active Directory. Identity Management for UNIX simplifies Windows-to-UNIX user account mapping management in Active Directory.
- Enhanced server performance—Microsoft Services for NFS includes a file filter driver, which significantly reduces common server file access latencies.
- UNIX special device support—Microsoft Services for NFS supports UNIX special devices (mknod).
- Enhanced UNIX support—Microsoft Services for NFS now supports the following versions of UNIX:
  - Hewlett Packard HP-UX version 11i
  - IBM AIX version 5L 5.2
  - Red Hat Linux version 9
  - Sun Microsystems Solaris version 9

The following features that were previously available in Services for UNIX 3.5 are not included in MSNFS:

- Gateway for NFS
- Server for PCNFS
- All PCNFS components of Client for NFS

UNIX Identity Management

Identity Management for UNIX makes it easy to integrate users of Windows operating systems into existing UNIX environments. It provides manageability components that simplify network administration and account management across both platforms.

With Identity Management for UNIX, the administrator can:

- Manage user accounts and passwords on Windows and UNIX systems using Network Information Service (NIS).
- Automatically synchronize passwords between Windows and UNIX operating systems.

UNIX Identity Management consists of the following components:

- Administration components
- Password synchronization
- Server for NIS

The UNIX Identity Management component is not enabled by default on the storage system. To install this component:

1. Access **Add/Remove Programs**.
2. Select **Add/Remove Windows Components > Active Directory Services > Details**.
3. Install **Identity Management for Windows**.

MSNFS use scenarios

The following use scenarios are supported by MSNFS file services:

- Allow UNIX clients to access resources on computers running Windows Server 2003 R2.

  Your company may have UNIX clients accessing resources, such as files, on UNIX file servers. To take advantage of new Windows Server 2003 features, such as Shadow Copies for Shared Folders, you can move resources from your UNIX servers to computers running Windows Server 2003 R2. You can then set up MSNFS to enable access by UNIX clients that are running NFS software. All of your UNIX clients will be able to access the resources using the NFS protocol with no changes required.

- Allow computers running Windows Server 2003 R2 to access resources on UNIX file servers.

  Your company may have a mixed Windows and UNIX environment with resources, such as files, stored on UNIX file servers. You can use MSNFS to enable computers running Windows Server 2003 R2 to access these resources when the file servers are running NFS software.

MSNFS components

MSNFS comprises the following three main components:

- Username Mapping Server

  Username Mapping Server maps user names between Windows and UNIX user accounts. In a heterogeneous network, users have separate Windows and UNIX security accounts. Users must provide a different set of credentials to access files and other resources, depending on whether they are stored on a Windows or UNIX file server. To address this issue, Username Mapping Server maps the Windows and UNIX user names so that users can log on with either their Windows or UNIX credentials and access resources regardless of whether they are stored on a Windows or UNIX file server.

- Server for NFS

  Normally, a UNIX computer cannot access files on a Windows-based computer. A computer running Windows Server 2003 R2 and Server for NFS, however, can act as a file server for both Windows and UNIX computers.

- Client for NFS

  Normally, a Windows-based computer cannot access files on a UNIX computer. A computer running Windows Server 2003 R2 and Client for NFS, however, can access files stored on a UNIX-based NFS server.

The Client for NFS feature of the Microsoft Services for NFS component is not preinstalled on the storage system although information about this feature appears in the online help. To enable Client for NFS:

1. Go to **Add/Remove Programs**.
2. Select **Add/Remove Windows Components > Other Network File and Print Services > Microsoft Services for NFS > Details**.
3. Install Client for NFS.

Administering MSNFS

To access Microsoft Services for Network File System from the Start menu:

1. Select **Start > Programs > Administrative Tools**.
2. Click **Microsoft Services for Network File System**.

To access Microsoft Services for Network File System from the HP All-in-One Management Console:

1. Access the HP All-in-One Management Console by clicking on the shortcut icon on the desktop.
2. In the left pane of the console, select the **Share Folder Management** listing.
3. In the center pane, under **Share Utilities**, select **Microsoft Services for NFS** .

Server for NFS

With Server for NFS, a computer running the Microsoft Windows Server 2003 R2 operating system can act as a Network File System (NFS) server. Users can then share files in a mixed environment of computers, operating systems, and networks. Users on computers running NFS client software can gain access to directories (called shares) on the NFS server by connecting (mounting) those directories to their computers. From the viewpoint of the user on a client computer, the mounted files are indistinguishable from local files.

UNIX computers follow advisory locking for all lock requests. This means that the operating system does not enforce lock semantics on a file, and applications that check for the existence of locks can use these locks effectively. However, Server for NFS implements mandatory locks even for those locking requests that are received through NFS. This ensures that locks acquired through NFS are visible through the server message block (SMB) protocol and to applications accessing the files locally. Mandatory locks are enforced by the operating system.

Server for NFS Authentication DLL vs. Service for User for Active Directory domain controllers

On a Windows Storage Server 2003 R2 storage system, Server for NFS depends on a domain controller feature called Service for User (S4U) to authenticate UNIX users as their corresponding Windows users. Windows Server operating systems prior to Windows Server 2003 and Windows Storage Server 2003 do not support S4U. Also, in mixed domain environments, legacy Services for UNIX (SFU), Services for NFS and Windows Storage Server 2003 NFS deployments do not use the S4U feature and still depend on the Server for NFS Authentication DLL being installed on domain controllers.

Therefore, the administrator needs to install the Server for NFS Authentication DLL on Windows 2000 domain controllers when:

- The NFS file serving environment uses previous NFS releases (NAS, SFU, and so on).
- The Windows domain environment uses pre-2003 domain controllers.

Refer to Table 47 for guidance as to when to use NFS Authentication DLL instead of S4U legacy NFS and R2 MSNFS.

Table 47 Authentication table

Domain controller type	Legacy NFS (pre-WSS2003 R2)	MSNFS (WSS2003 R2)
Legacy domain controller (pre-WSS2003)	Requires NFS Authentication DLL on domain controller	Requires NFS Authentication DLL on domain controller
Recent domain controllers (WSS2003 and later)	Requires NFS Authentication DLL on domain controller	Uses the built-in S4U (on the domain controller). It is unaffected by the NFS Authentication DLL on the domain controller.

The S4U set of extensions to the Kerberos protocol consists of the Service-for-User-to-Proxy (S4U2Proxy) extension and the Service-for-User-to-Self (S4U2Self) extension. For more information about the S4U2 extensions, see the Kerberos articles at the following URLs: http://searchwindowssecurity.techtarget.com/originalContent/0,289142,sid45_gci1013484,00.html (intended for IT professionals) and http://msdn.microsoft.com/msdnmag/issues/03/04/SecurityBriefs/default.aspx (intended for developers).

Installing NFS Authentication DLL on domain controllers

NOTE:

If the authentication software is not installed on all domain controllers that have user name mappings, including primary domain controllers, backup domain controllers, and Active Directory domains, then domain user name mappings will not work correctly.

You need to install the version of NFS Authentication included with Services for UNIX 3.5. You can download Services for UNIX 3.5 at no charge from http://go.microsoft.com/fwlink/?LinkId=44501.

To install the Authentication software on the domain controllers:

1. From the SFU 3.5 files, locate the directory named `SFU35SEL_EN`.
2. On the domain controller where the Authentication software is being installed use Windows Explorer to:
   a. Open the shared directory containing `setup.exe`.
   b. Double-click the file to open it. Windows Installer is opened.

NOTE:

If the domain controller used does not have Windows Installer installed, locate the file `InstMSI.exe` on the SFU 3.5 directory and run it. After this installation, the Windows Installer program starts when opening `setup.exe`.

3. In the Microsoft Windows Services for UNIX Setup Wizard dialog box, click **Next**.
4. In the User name box, enter your name. If the name of your organization does not appear in the Organization box, enter the name of your organization there.

5. Read the End User License Agreement carefully. If you accept the terms of the agreement, click **I accept the terms in the License Agreement**, and then click **Next** to continue installation. If you click **I do not accept the License Agreement** (Exit Setup), the installation procedure terminates.
6. Click Custom Installation, and then click **Next**.
7. In the Components pane, click the down arrow next to Windows Services for UNIX, and then click **Entire component will not be available**.
8. Click the plus sign (+) next to Authentication Tools.
9. In the Components pane, click the plus sign (+) next to Authentication Tools.
10. Click **Server for NFS Authentication**, click **Will be installed on local hard drive**, and then click **Next**.
11. Follow the remaining instructions in the wizard.

NOTE:

NFS users can be authenticated using either Windows domain accounts or local accounts on the Windows server. Server for NFS Authentication must be installed on all domain controllers in the domain if NFS users will be authenticated using domain accounts. Server for NFS Authentication is always installed on the computer running Server for NFS.

Elevate S4U2 functionality on Windows Server 2003 domain controllers

NOTE:

The S4U2 functionality does not work until the domain functional level is elevated to Windows Server 2003.

To elevate the functional level to Windows Server 2003:

1. On the Windows 2003 domain controller, open Active Directory Domains and Trusts.
2. In the console tree, right-click the domain for which you want to raise functionality, and then click **Raise Domain Functional Level**.
3. In Select an available domain functional level, click **Windows Server 2003**.
4. Click **Raise**.

Server for NFS administration

The Server for NFS administration online help contains information for the following topics:

- Understanding the Server for NFS component
- Starting and stopping Server for NFS
- Configuring Server for NFS
- Securing Server for NFS
- Optimizing Server for NFS performance
- Using file systems with NFS
- Managing NFS shares
- Managing NFS client groups
- Server for NFS Authentication

Accessing NFS resources for Windows users and groups

Server for NFS allows Windows clients to access NFS resources on the storage system without separately logging on to Server for NFS. The first time users attempt to access an NFS resource, the Server for NFS looks up the user's UNIX UID and GID information in either Windows Active Directory or the User Name Mapping function on the storage system. If the UNIX UID and GID information is mapped to a Windows user and group accounts, the Windows names are returned to Server for NFS, which then uses the Windows user and group names to grant file access. If the UNIX UID and GID information is not mapped, then Server for NFS will deny file access.

There are two ways to specify how Server for NFS on the storage system obtains Windows user and group information:

- Using the Windows interface
- Using a command line (`nfsadmin.exe`)

IMPORTANT:

- Before using Active Directory Lookup, administrators must install and populate the Identity Management for UNIX Active Directory schema extension, included in Windows Server 2003 R2, or have an equivalent schema which includes UNIX UID and GID fields.
- The IP address of the User Name Mapping server can be specified instead of the name of the server.
- Before using User Name Mapping, the computer running Server for NFS must be listed in the .maphosts file on the computer running User Name Mapping. For more information, see "Securing access to the User Name Mapping server."

For additional information about accessing NFS resources, see the MSNFS online help. For additional information about Identity Management for UNIX, see the UNIX Identify Management online help

Managing access using the .maphosts file

The User Name Mapping component of MSNFS acts as an intermediary between NFS servers and NFS clients on a network containing UNIX hosts and Windows-based computers. To maintain the implicit trust relationship between NFS client and host computers, administrators can control which computers can access User Name Mapping by editing the .maphosts in the %windir%\msnfs directory of the storage system. Conditions to allow or deny access include:

- If the .maphosts file is present but not empty, then only those computers allowed access by entries in the file can access User Name mapping.
- If the .maphosts file is present but empty (the default), no computers except the computer running User Name Mapping itself can access User Name Mapping.
- If the .maphosts file is not present, no computers (including the computer running User Name Mapping) can access User Name Mapping.

The ordering of entries is important as User Name Mapping searches the .maphosts file from the top down until it finds a match.

For additional information about the .maphosts file, see the MSNFS online help.

Allowing anonymous access to resources by NFS clients

It may be desirable to add anonymous access to a share. An instance would be when it is not desirable or possible to create and map a UNIX account for every Windows user. A UNIX user whose account

is not mapped to a Windows account is treated by Server for NFS as an anonymous user. By default, the user identifier (UID) and group identifier (GID) is -2.

For example, if files are created on an NFS Share by UNIX users who are not mapped to Windows users, the owner of those files are listed as anonymous user and anonymous group, (-2,-2).

By default, Server for NFS does not allow anonymous users to access a shared directory. When an NFS share is created, the anonymous access option can be added to the NFS share. The values can be changed from the default anonymous UID and GID values to the UID and GID of any valid UNIX user and group accounts.

NOTE:

In Windows Server 2003, the Everyone group does not include anonymous users by default.

When allowing anonymous access to an NFS Share, the following must be performed by a user with administrative privileges due to Windows Storage Server 2003 security with anonymous users and the Everyone group.

1. Click **Remote Desktop**. Log on to the storage system.
2. Click **Start** >**Control Panel** > **Administrative Tools**, and then click **Local Security Policy**.
3. In Security Settings, double-click **Local Policies**, and then click **Security Options**.
4. Right-click **Network access: Let Everyone permissions apply to anonymous users**, and then click **Properties**.
5. To allow permissions applied to the Everyone group to apply to anonymous users, click **Enabled**. The default is **Disabled**.
6. Restart the NFS server service. From a command prompt, enter `net stop nfssvc`. Then enter `net start nfssvc`. Notify users before restarting the NFS service.
7. Assign the Everyone group the appropriate permissions on the NFS Share.
8. Enable anonymous access to the share.

To enable anonymous access to an NFS share:

1. Open Windows Explorer by clicking **Start** > **Run**, and entering Explorer.
2. Navigate to the NFS share.
3. Right-click the NFS Share, and then click **Properties**.
4. Click **NFS Sharing**.
5. Select the **Allow Anonymous Access** checkbox.
6. Change from the default of -2,-2, if desired.
7. Click **Apply**.
8. Click **OK**.

Best practices for running Server for NFS

- Provide user-level security
- Secure files
- Secure new drives
- Allow users to disconnect before stopping the Server for NFS service

- Use naming conventions to identify shares with EUC encoding
- Protect configuration files

For further details, see the online help for Microsoft Services for Network File System.

User Name Mapping

The User Name Mapping component provides centralized user mapping services for Server for NFS and Client for NFS. User Name Mapping lets you create maps between Windows and UNIX user and group accounts even though the user and group names in both environments may not be identical. User Name Mapping lets you maintain a single mapping database making it easier to configure account mapping for multiple computers running MSNFS.

In addition to one-to-one mapping between Windows and UNIX user and group accounts, User Name Mapping permits one-to-many mapping. This lets you associate multiple Windows accounts with a single UNIX account. This can be useful, for example, when you do not need to maintain separate UNIX accounts for individuals and would rather use a few accounts to provide different classes of access permission.

You can use simple maps, which map Windows and UNIX accounts with identical names. You can also create advanced maps to associate Windows and UNIX accounts with different names, which you can use in conjunction with simple maps.

User Name Mapping can obtain UNIX user, password, and group information from one or more Network Information Service (NIS) servers or from password and group files located on a local hard drive. The password and group files can be copied from a UNIX host or from a NIS server.

User Name Mapping periodically refreshes its mapping database from the source databases, ensuring that it is always kept up-to-date as changes occur in the Windows and UNIX name spaces. You can also refresh the database anytime you know the source databases have changed.

You can back up and restore User Name Mapping data at any time. Because the database is backed up to a file, you can use that file to copy the mapping database to another server. This provides redundancy for the sake of fault tolerance.

NOTE:

If you obtain information from multiple NIS domains, it is assumed that each domain has unique users and user identifiers (UIDs). User Name Mapping does not perform any checks.

User Name Mapping associates Windows and UNIX user names for Client for NFS and Server for NFS. This allows users to connect to Network File System (NFS) resources without having to log on to UNIX and Windows systems separately.

NOTE:

Most of the functionality of User Name Mapping has been replaced by Active Directory Lookup. Active Directory Lookup enables Client for NFS and Server for NFS to obtain user identifier (UID) and group identifier (GID) information directly from Active Directory. For information about storing UNIX user data in Active Directory, see documentation for Identity Management for UNIX. For information about enabling Active Directory Lookup, see “Specifying how Server for NFS obtains Windows user and group information” available in online help.

User Name Mapping Administration

The User Name Mapping administration online help contains information for the following topics:

- Understanding the User Name Mapping component
- Starting and stopping User Name Mapping
- Configuring User Name Mapping
- Securing access to the User Name Mapping server
- Managing maps
- Managing groups

Best practices for User Name Mapping

- Install User Name Mapping on a domain controller.
- Create a User Name Mapping server pool.
- Make sure User Name Mapping can download users from all domains.
- Refresh data whenever a user is added or changed.
- Place password and group files on the User Name Mapping server.
- Use appropriate permissions to protect password and group files.
- Ensure consistency of group mapping.
- Specify the computers that can access User Name Mapping.

For further details, see the online help for Microsoft Services for Network File System.

Microsoft Services for NFS troubleshooting

The following information on how to troubleshoot issues with Microsoft Services for NFS is available using the online help:

- General issues
- Troubleshooting Server for NFS
- Troubleshooting User Name Mapping

For further details, see the online help for Microsoft Services for Network File System.

Microsoft Services for NFS command-line tools

Table 48 provides a listing of Windows command-line administration tools.

Table 48 MSNFS command-line administration tools

Command	Function
mapadmin	Adds, lists, deletes, or changes user name mappings
mount	Mounts NFS network exports (shares)
nfsadmin	Manages Server for NFS and Client for NFS
nfsshare	Displays, adds, and removes exported NFS shares
nfsstat	Views statistics by NFS operation type
showmount –a	Views users who are connected and what the user currently has mounted

Command	Function
showmount –e	Views exports from the server and their export permissions
unmount	Removes NFS-mounted drives

For further details, see the online help for Microsoft Services for Network File System.

Optimizing Server for NFS performance

The following sources provide useful information on how to optimize performance for Microsoft Services for NFS.

The MSNFS online help covers the following topic areas:

- Adding performance counters
- Monitoring and tuning performance
- Changing the directory cache memory setting

For further details, see the online help for Microsoft Services for Network File System.

A technical paper titled *Performance Tuning Guidelines for Microsoft Services for Network File System* is available at http://www.microsoft.com/technet/interopmigration/unix/sfu/perfnfs.mspx.

Print services for UNIX

Network clients with UNIX-based operating systems that use the client program line printer remote (LPR) can send printing jobs to the line printer daemon (LPD) on the storage system. LPR clients must comply with Request for Comments (RFC) 1179. The combination of the LPR and LPD are included in print services for UNIX. Print services for UNIX is not preinstalled on the print server or the File Print Appliance.

To install print services for UNIX:

1. Log on as administrator or as a member of the Administrators group.
2. Select **Start** > **Control Panel**, and then click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. In the Components list, click **Other Network File and Print Services** (but do not select or clear the check box), and then click **Details**.
5. In the Subcomponents of Other Network File and Print Services list, select **Print Services for UNIX**, if appropriate to the print services that you want to install:

   Print Services for UNIX: This option permits UNIX clients to print to any printer that is available to the print server.

   NOTE:

   When installing Print Services for UNIX, this automatically installs the LPR port and the TCP/IP Print Server service.

6. Click **OK**, and then click **Next**.
7. Click **Finish**.

Point and print from UNIX to Windows Server 2003

Point-and-Print behavior from UNIX clients to Windows Server 2003 and Windows Storage Server 2003 is similar to the behavior for Windows 95, Windows 98, and Windows Millennium Edition clients, because all these clients create SMB connections. However, the non–Windows operating systems maintain their own driver model, so these clients do not automatically get the driver during Point and Print—they must install the driver locally. Like the Windows 95, Windows 98, and Windows Millennium clients, these non–Windows clients do not receive driver updates from the print server after a driver is initially downloaded. The same connection methods are available: drag and drop, the Add Printer Wizard, referencing a UNC path, or double-clicking the shared printer icon.

Additional resources

Consult the following resources for more information about using and configuring Print Services for UNIX:

- How To: Install and Configure Print Services for UNIX
  http://support.microsoft.com/kb/324078
- How To: Install Print Services for UNIX in Windows Server 2003
  http://support.microsoft.com/?scid=kb;en-us;323421

D Other network file and print services

This chapter discusses file and print services for NetWare and Macintosh.

File and Print Services for NetWare (FPNW)

File and Print Services for NetWare (FPNW) is one part of the Microsoft software package called Services for NetWare. The most common use of the NetWare network operating system is as a file and print server. FPNW eases the addition of the storage system into a mixed infrastructure by providing a NetWare user interface (UI) to a Windows Storage Server 2003-based server; administrators and users see their same, familiar NetWare UI. Additionally, the same logon for clients is maintained without a need for any client configuration changes.

This service also provides the ability to create Novell volumes, which are actually NTFS shares, from which users can map drives and access resources. Novell Login scripts are supported on the storage system or through an existing NDS (Novell Directory Services) account. This requires no changes or additions to the software on the NetWare client computers.

NOTE:

IPX/SPX protocol is required on the Novell servers.

Installing Services for NetWare

The installation of FPNW on the storage system allows for a smooth integration with existing Novell servers. FPNW allows a Windows Storage Server 2003 based server to emulate a NetWare file and print server to users, clients, and administrators. This emulation allows authentication from Novell clients, the use of Novel logon scripts, the creation of Novell volumes (shares), the use of Novell file attributes, and many other Novell features.

Information on Microsoft Directory Synchronization Services and the File Migration Utility can be found at

http://www.microsoft.com/WINDOWS2003/guide/server/solutions/NetWare.asp

To install Services for NetWare:

1. From the desktop of the storage system, select **Start** > **Settings** > **Network Connections > Local Area Connection**, and then right-click **Properties**.
2. Click **Install**.

   The **Select Network Component Type** dialog box is displayed.
3. Click **Service**, and then click **Add**.
4. Click the **Have Disk** icon, and then navigate to the location of **Services for NetWare**.

   Services for NetWare is located in the path:
   `c:\hpnas\components\SFN5.02\fpnw\netsfn.inf`.

5. Select the `NETSFNTSRV` file, and then click **OK**.

   File and Print Services for NetWare should now be displayed as an option to install.

6. Select **File and Print Services for NetWare**, and then click **OK**.

Managing File and Print Services for NetWare

FPNW resources are managed through Server Manager. Server Manager can be used to modify FPNW properties and manager shared volumes.

Use File and Print Services for NetWare to:

- Access files, modify file settings and permissions from Computer Management, and use third party tools that can be used with NetWare servers.
- Create and manage user accounts by using Active Directory Users and Computers.
- Perform secured log-ons.
- Support packet burst and Large Internet Packet (LIP).
- Support NetWare locking and synchronization primitives that are used by some NetWare-specific applications.
- Support long file names, compatible with OS/2 long file name (LFN) support.

File and Print Services for NetWare does not support the following NetWare groups and functions:

- Workgroup Managers
- Accounting
- User disk volume restrictions
- Setting Inherited Rights Masks (IRMs)
- NetWare loadable modules
- Transaction Tracking System (TTS)

To access File and Print Services:

To access FPNW:

1. From the desktop of the storage system, select **Start** > **Settings** > **Control Panel > Administrative Tools > Server Manager**.

2. Select **FPNW**, and then click **Properties**.

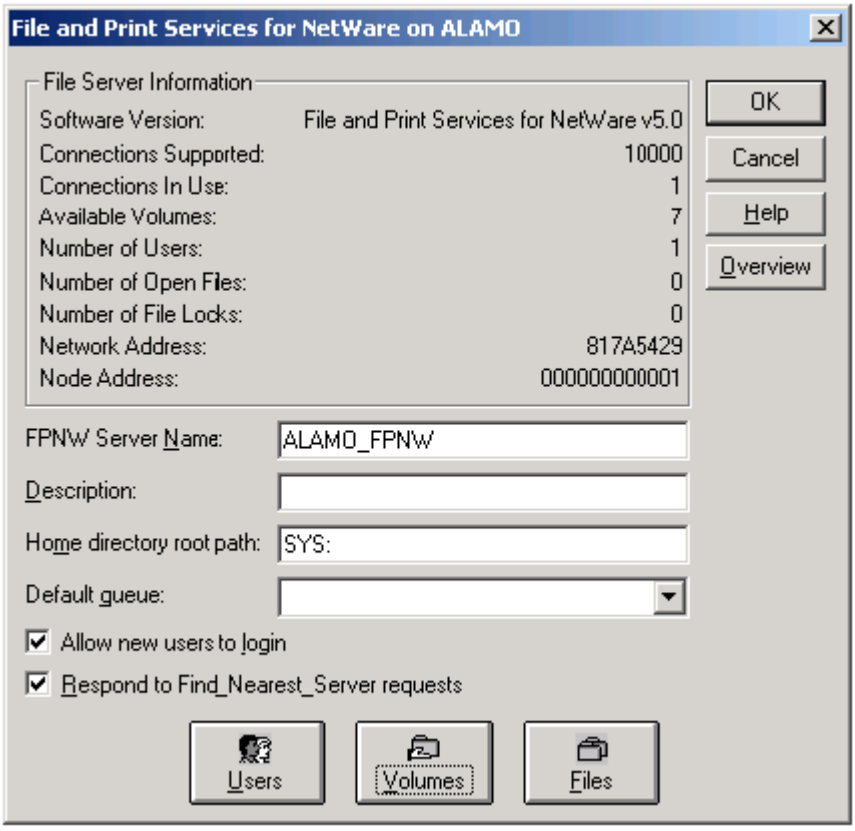


Figure 32 File and Print Services for NetWare dialog box

3. Enter an FPNW Server Name and Description.

   This server name must be different from the server name used by Windows or LAN Manager-based clients. If changing an existing name, the new name is not effective until stopping and restarting FPNW. For example, in Figure 32 the Windows server name is Alamo and the FPNW server name is Alamo_FPNW.

4. Indicate a Home directory root path.

   This path is relative to where the Sysvol volume is installed. This is the root location for the individual home directories. If the directory specified does not already exist, it must first be created.

5. Click **Users** to:

   See connected users, disconnect users, send broadcast messages to all users connected to the server, and to send a message to a specific user.

6. Click **Volumes** to:

   See users connected to specific volume and to disconnect users from a specific volume.

7. Click **Files** to:

   View open files and close open files.

Creating and managing NetWare users

To use Services for NetWare, the Novell clients must be entered as local users on the storage system.

Adding local NetWare users

1. From the storage system desktop, click the **Management Console** icon, click **Core Operating System**, and then click **Local Users and Groups**.
2. Right-click the **Users** folder, and then click **New User**.

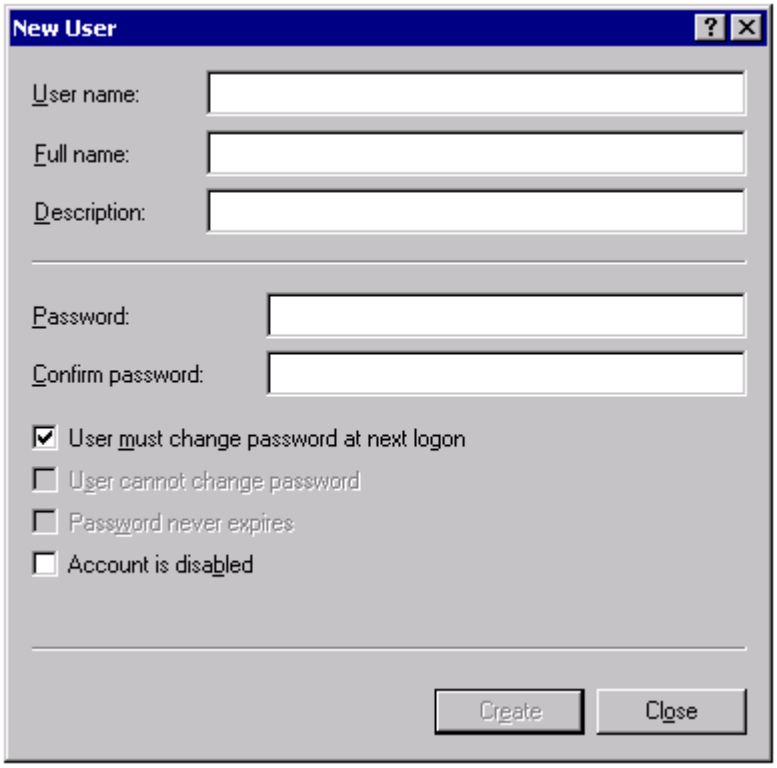


Figure 33 New User dialog box

3. Enter the user information, including the user's User name, Full name, Description, and Password.
4. Click **Create**.
5. Repeat these steps until all NetWare users have been entered.

Enabling local NetWare user accounts

1. In the **Users** folder (MC, Core Operating System, Local Users and Groups), right-click an NCP client listed in the right pane of the screen, and then click **Properties**.

2. Click the **NetWare Services** tab.

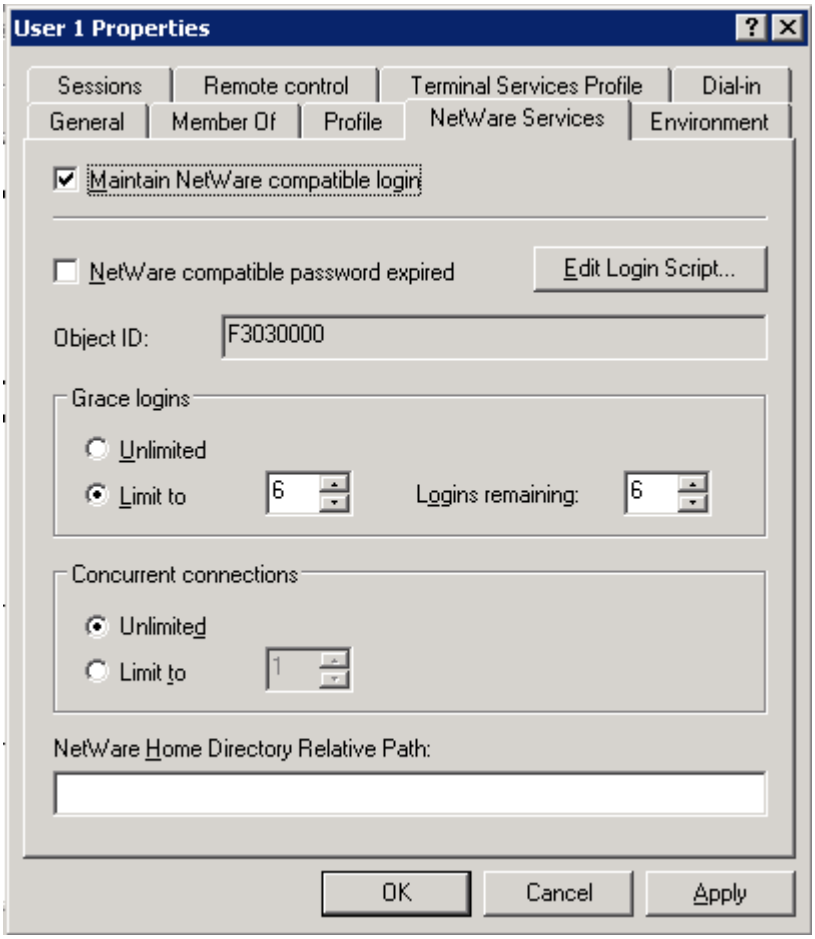


Figure 34 NetWare Services tab

3. Select **Maintain NetWare compatible login**.
4. Set other NetWare options for the user, and then click **OK**.

NOTE:

The installation of File and Print Services for NetWare also creates a supervisor account, which is used to manage FPNW. The supervisor account is required if the storage system was added as a bindery object into NDS.

Managing NCP volumes (shares)

NCP file shares are created the same way as other file shares; however, there are some unique settings. NCP shares can be created and managed using Server Manager.

NOTE:

NCP shares can be created only after FPNW is installed. See the previous section "Installing Services for Netware" for instructions on installing FPNW.

Creating a new NCP share

To create a new file share:

1. From the storage system desktop, select **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Server Manager**.
2. Select **File and Print Service for NetWare**> **Shared Volumes**.
3. Click **Create Volume**.
4. Specify the volume name and path.
5. Click **Permissions** to set permissions.
6. Click **Add** to add additional users and groups, and to set their permissions.
7. Highlight the desired user or group, and then click **Add**.
8. Select the Type of Access in the drop down list.

   Type of Access can also be set from the Access Through Share Permissions dialog box.
9. Click **OK** when all users and groups have been added.
10. Click **OK** in the **Create Volume** dialog box.
11. Click **Close**.

Modifying NCP share properties

To modify a file share:

1. From the storage system desktop, select **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Server Manager**.
2. Select **File and Print Services for NetWare** > **Shared Volumes**.
3. Highlight the volume to modify.
4. Click **Properties**.

Print Services for NetWare

With File and Print Services for NetWare installed, the print server or File Print Appliance appears to a NetWare client as a NetWare 3.x–compatible print server. Print services presents the same dialog boxes to the client as a NetWare-based server uses to process a print job from a client. A user can display and search for printers on the print server or File Print Appliance just like in a NetWare environment.

Installing Print Services for NetWare

Refer to the previous section "Installing Services for Netware" for information on installing Print Services for NetWare.

Point and Print from Novell to Windows Server 2003

Point-and-Print behavior from Novell clients to Windows Server 2003 and Windows Storage Server 2003 is similar to the behavior for Windows 95, Windows 98, and Windows Millennium Edition clients, because all these clients create SMB connections. However, the non–Windows operating systems maintain their own driver model, so these clients do not automatically get the driver during

Point and Print—they must install the driver locally. Like the Windows 95, Windows 98, and Windows Millennium clients, these non–Windows clients do not receive driver updates from the print server after a driver is initially downloaded. The same connection methods are available: drag and drop, the Add Printer Wizard, referencing a UNC path, or double-clicking the shared printer icon.

Additional resources

For more information about using and configuring File and Print Services for NetWare, see the online help.

AppleTalk and file services for Macintosh

The AppleTalk network integration allows the storage system to share files and printers between your server and any Apple Macintosh clients that are connected to your network. After installing Microsoft Windows Services for Macintosh, the administrator can use the AppleTalk protocol to configure the storage system to act as an AppleTalk server. The AppleTalk protocol is the communications protocol used by clients running a Macintosh operating system. The Macintosh computers need only the Macintosh OS software to function as clients; no additional software is required.

AppleTalk network integration simplifies administration by maintaining just one set of user accounts instead of separate user accounts, for example, one on the Macintosh server and another on the computer running Windows server software.

Installing the AppleTalk protocol

1. From the desktop of the storage system, select **Start>Settings > Network Connections**. Right-click **Local Area Connection**, and then click **Properties**.
2. Click **Install**.
3. Select **Protocol**, and then click **Add**.
4. Select **AppleTalk Protocol**, and then click **OK**.

Installing File Services for Macintosh

To install File Services for Macintosh, perform the following steps:

1. Access the desktop on the storage system.
2. Open **Add or Remove Programs** from the Control Panel.
3. Click **Add or Remove Windows Components**.
4. Double-click **Other Network File and Print Services**.
5. Select **File Services for Macintosh**, and then click **OK**.
6. Click **Next**.
7. Click **Finish**.

Completing setup of AppleTalk protocol and shares

See the online help to complete the following set up and configurations tasks:

- To set up AppleTalk protocol properties

AppleTalk shares can be set up only after AppleTalk Protocol and File Services for Macintosh have been installed on the storage system.

△ CAUTION:

AppleTalk shares should not be created on clustered resources because data loss can occur due to local memory use.

- To set up AppleTalk shares
- To configure AppleTalk sharing properties
- To allow client permission to an AppleTalk share

  If AppleTalk is enabled for your server configuration, specify which AppleTalk clients are granted access to each share. Access can be granted or denied on the basis of client host name. Access can also be granted or denied on the basis of client groups, where a client group contains one or more client host names.

Print services for Macintosh

Macintosh clients can send print jobs to a print server or File Print Appliance (FPA) when Print Server for Macintosh is installed on the server. To the Macintosh-based client, the print server or FPA appears to be an AppleTalk printer on the network, and no reconfiguration of the client is necessary.

Installing Print Services for Macintosh

Consult the following resource for information about installing Print Services for Macintosh:

- How To: Install Print Services for Macintosh in Windows Server 2003
  http://support.microsoft.com/?scid=kb;en-us;323421

Point and Print from Macintosh to Windows Server 2003

Point-and-Print behavior from Macintosh clients to Windows Server 2003 or Windows Storage Server 2003 is similar to the behavior for Windows 95, Windows 98, and Windows Millennium Edition clients, because all these clients create SMB connections. However, the non-Windows operating systems maintain their own driver model, so these clients do not automatically get the driver during Point and Print—they must install the driver locally. Like the Windows 95, Windows 98, and Windows Millennium clients, these non-Windows clients do not receive driver updates from the print server after a driver is initially downloaded. The same connection methods are available: drag and drop, the Add Printer Wizard, referencing a UNC path, or double-clicking the shared printer icon.

E Configuring storage system for Web access (optional)

Setting up an Internet connection

Before running Windows 2003 R2 operating system updates, you must set up an Internet connection for the storage system. There are two methods for configuring an Internet connection:

- Internet Explorer to use automatic configuration
- Internet Explorer to use a proxy server

To configure Internet Explorer to use automatic configuration

1. On the **Tools** menu in Internet Explorer, click **Internet Options**, click the **Connections** tab, and then click **LAN Settings**.
2. Under **Automatic Configuration**, click either the **Automatically detect settings** or **Use automatic configuration script** check box.

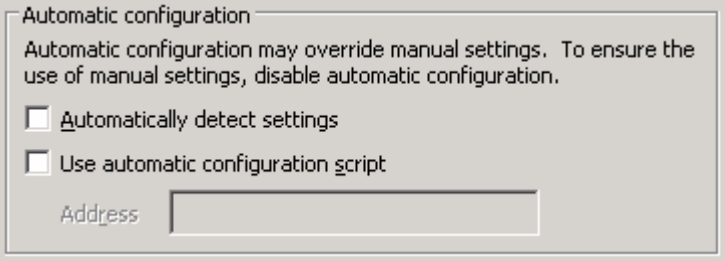

Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address

Figure 35 Automatic configuration settings

3. Click **OK** to close the **LAN Settings** dialog box.
4. Click **OK** again to close the **Internet Options** dialog box.

To configure Internet Explorer to use a proxy server

1. On the **Tools** menu in Internet Explorer, click **Internet Options**, click the **Connections** tab, and then click **LAN Settings**.
2. Under **Proxy server**, click the **Use a proxy server for your LAN** check box.

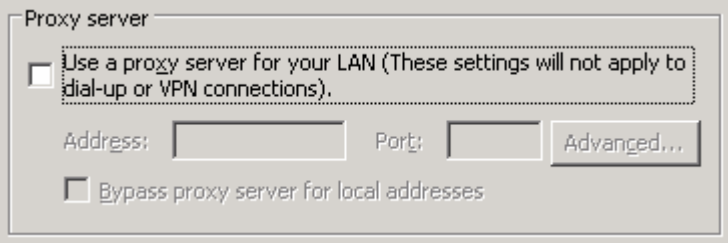

Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
Port:
Advanced...
Bypass proxy server for local addresses

Figure 36 Proxy server settings

3. In the **Address** box, type the network name or IP address of the proxy server.
4. In the **Port** box, type the port number that is used by the proxy server for client connections (for example, 8080).
5. Click the **Bypass proxy server for local addresses** check box if you do not want the proxy server computer to be used when you connect to a computer on the local network.
6. Click **OK** to close the **LAN Settings** dialog box.
7. Click **OK** again to close the **Internet Options** dialog box.

F Regulatory compliance and safety

Federal Communications Commission notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (personal computers, for example). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows which class (A or B) the equipment falls into. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or FCC ID on the label. Once the class of the device is determined, refer to the following corresponding statement.

Class A equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

Declaration of conformity for products marked with the FCC logo, United States only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding your product, contact:

Hewlett-Packard Company

P. O. Box 692000, Mail Stop 530113

Houston, Texas 77269-2000

Or, call

1-800- 652-6672

For questions regarding this FCC declaration, contact:

Hewlett-Packard Company

P. O. Box 692000, Mail Stop 510101

Houston, Texas 77269-2000

Or, call

(281) 514-3333

To identify this product, refer to the Part, Series, or Model number found on the product.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Company may void the user's authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Laser compliance

This product may be provided with an optical storage device (that is, CD or DVD drive) and/or fiber optic transceiver. Each of these devices contains a laser that is classified as a Class 1 Laser Product in accordance with US FDA regulations and the IEC 60825–1. The product does not emit hazardous laser radiation.

⚠ WARNING!

Use of controls or adjustments or performance of procedures other than those specified herein or in the installation guide of the laser product may result in hazardous radiation exposure. To reduce the risk of exposure to hazardous radiation:

- Do not try to open the module enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only HP authorized service technicians to repair the unit.

The Center for Devices and Radiological Health (CDRH) of the U.S. Food and Drug Administration implemented regulations for laser products on August 2, 1976. These regulations apply to laser products manufactured from August 1, 1976. Compliance is mandatory for products marketed in the United States.

International notices and statements

Canadian notice (Avis Canadien)

Class A equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union notice

CE Products bearing the CE marking comply with the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community and if this product has telecommunication functionality, the R&TTE Directive (1999/5/EC).

Compliance with these directives implies conformity to the following European Norms (in parentheses are the equivalent international standards and regulations):

- EN 55022 (CISPR 22) - Electromagnetic Interference
- EN55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11) - Electromagnetic Immunity
- EN61000-3-2 (IEC61000-3-2) - Power Line Harmonics
- EN61000-3-3 (IEC61000-3-3) - Power Line Flicker
- EN 60950 (IEC 60950) - Product Safety

BSMI notice

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Japanese notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です　この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean notice A&B

Class A equipment

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Class B equipment

B급 기기 (가정용 정보통신기기)

이 기기는 가정용으로 전자파적합등록을 한 기기로서 주거지역에서는 물론 모든지역에서 사용할 수 있습니다.

Safety

Battery replacement notice

⚠ WARNING!

The computer contains an internal lithium manganese dioxide, a vanadium pentoxide, or an alkaline battery pack. A risk of fire and burns exists if the battery pack is not properly handled. To reduce the risk of personal injury:

- Do not attempt to recharge the battery.
- Do not expose the battery to temperatures higher than 60°C (140°F).
- Do not disassemble, crush, puncture, short external contacts, or dispose of in fire or water.

Batteries, battery packs, and accumulators should not be disposed of together with the general household waste. To forward them to recycling or proper disposal, please use the public collection system or return them to HP, an authorized HP Partner, or their agents.

For more information about battery replacement or proper disposal, contact an authorized reseller or an authorized service provider.

Taiwan battery recycling notice

The Taiwan EPA requires dry battery manufacturing or importing firms in accordance with Article 15 of the Waste Disposal Act to indicate the recovery marks on the batteries used in sales, giveaway or promotion. Contact a qualified Taiwanese recycler for proper battery disposal.

Power cords

The power cord set must meet the requirements for use in the country where the product was purchased. If the product is to be used in another country, purchase a power cord that is approved for use in that country.

The power cord must be rated for the product and for the voltage and current marked on the product electrical rating label. The voltage and current rating of the cord should be greater than the voltage and current rating marked on the product. In addition, the diameter of the wire must be a minimum of 1.00 mm^2 or 18 AWG, and the length of the cord must be between 1.8 m (6 ft) and 3.6 m (12 ft). If you have questions about the type of power cord to use, contact an HP authorized service provider.

NOTE:

Route power cords so that they will not be walked on and cannot be pinched by items placed upon or against them. Pay particular attention to the plug, electrical outlet, and the point where the cords exit from the product.

Japanese power cord notice

製品には、同梱された電源コードをお使い下さい。
同梱された電源コードは、他の製品では使用出来ません。

Electrostatic discharge

To prevent damage to the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

Preventing electrostatic discharge

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the ground cords. To provide proper grounding, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part.

NOTE:

For more information on static electricity, or for assistance with product installation, contact your authorized reseller.

Waste Electrical and Electronic Equipment (WEEE) directive

Czechoslovakian notice

Likvidace za ízení soukromými domácími uživateli v Evropské unii

Tento symbol na produktu nebo balení ozna uje výrobek, který nesmí být vyhozen spolu s ostatním domácím odpadem. Povinností uživatele je p edat takto ozna ený odpad na p edem ur ené sb rné místo pro recyklaci elektrických a elektronických za ízení. Okamžité t íd ní a recyklace odpadu pom že uchovat p írodní prost edí a zajistí takový zp sob recyklace, který ochrání zdraví a životní prost edí lov ka. Další informace o možnostech odevzdání odpadu k recyklaci získáte na p íslušném obecním nebo m stském ú ad , od firmy zabývající se sb rem a svozem odpadu nebo v obchod , kde jste produkt zakoupili.

Danish notice

Bortskaffelse af affald fra husstande i den Europæiske Union

Hvis produktet eller dets emballage er forsynet med dette symbol, angiver det, at produktet ikke må bortskaffes med andet almindeligt husholdningsaffald. I stedet er det dit ansvar at bortskaffe kasseret udstyr ved at aflevere det på den kommunale genbrugsstation, der forestår genvinding af kasseret elektrisk og elektronisk udstyr. Den centrale modtagelse og genvinding af kasseret udstyr i forbindelse med bortskaffelsen bidrager til bevarelse af naturlige ressourcer og sikrer, at udstyret genvindes på en måde, der beskytter både mennesker og miljø. Yderligere oplysninger om, hvor du kan aflevere kasseret udstyr til genvinding, kan du få hos kommunen, den lokale genbrugsstation eller i den butik, hvor du købte produktet.

Dutch notice

Verwijdering van afgedankte apparatuur door privé-gebruikers in de Europese Unie

Dit symbool op het product of de verpakking geeft aan dat dit product niet mag worden gedeponeerd bij het normale huishoudelijke afval. U bent zelf verantwoordelijk voor het inleveren van uw afgedankte apparatuur bij een inzamelingspunt voor het recyclen van oude elektrische en elektronische apparatuur. Door uw oude apparatuur apart aan te bieden en te recyclen, kunnen natuurlijke bronnen worden behouden en kan het materiaal worden hergebruikt op een manier waarmee de volksgezondheid en het milieu worden beschermd. Neem contact op met uw gemeente, het afvalinzamelingsbedrijf of de winkel waar u het product hebt gekocht voor meer informatie over inzamelingspunten waar u oude apparatuur kunt aanbieden voor recycling.

English notice

Disposal of waste equipment by users in private household in the European Union

This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service, or the shop where you purchased the product.

Estonian notice

Seadmete jäätmete kõrvaldamine eramajapidamistes Euroopa Liidus

See tootel või selle pakendil olev sümbol näitab, et kõnealust toodet ei tohi koos teiste majapidamisjäätmetega kõrvaldada. Teie kohus on oma seadmete jäätmed kõrvaldada, viies need elektri- ja elektroonikaseadmete jäätmete ringlussevõtmiseks selleks ettenähtud kogumispunkti. Seadmete jäätmete eraldi kogumine ja ringlussevõtmine kõrvaldamise ajal aitab kaitsta loodusvarasid ning tagada, et ringlussevõtmine toimub viisil, mis kaitseb inimeste tervist ning keskkonda. Lisateabe saamiseks selle kohta, kuhu oma seadmete jäätmed ringlussevõtmiseks viia, võtke palun ühendust oma kohaliku linnakantselei, majapidamisjäätmete kõrvaldamise teenistuse või kauplusega, kust Te toote ostsite.

Finnish notice

Laitteiden hävittäminen kotitalouksissa Euroopan unionin alueella

Jos tuotteessa tai sen pakkauksessa on tämä merkki, tuotetta ei saa hävittää kotitalousjätteiden mukana. Tällöin hävitettävä laite on toimitettava sähkölaitteiden ja elektronisten laitteiden kierrätyspisteeseen. Hävitettävien laitteiden erillinen käsittely ja kierrätys auttavat säästämään luonnonvaroja ja varmistamaan, että laite kierrätetään tavalla, joka estää terveyshaitat ja suojelee luontoa. Lisätietoja paikoista, joihin hävitettävät laitteet voi toimittaa kierrätettäväksi, saa ottamalla yhteyttä jätehuoltoon tai liikkeeseen, josta tuote on ostettu.

French notice

Élimination des appareils mis au rebut par les ménages dans l'Union européenne

Le symbole apposé sur ce produit ou sur son emballage indique que ce produit ne doit pas être jeté avec les déchets ménagers ordinaires. Il est de votre responsabilité de mettre au rebut vos appareils en les déposant dans les centres de collecte publique désignés pour le recyclage des équipements électriques et électroniques. La collecte et le recyclage de vos appareils mis au rebut indépendamment du reste des déchets contribue à la préservation des ressources naturelles et garantit que ces appareils seront recyclés dans le respect de la santé humaine et de l'environnement. Pour obtenir plus d'informations sur les centres de collecte et de recyclage des appareils mis au rebut, veuillez contacter les autorités locales de votre région, les services de collecte des ordures ménagères ou le magasin dans lequel vous avez acheté ce produit.

German notice

Entsorgung von Altgeräten aus privaten Haushalten in der EU

Das Symbol auf dem Produkt oder seiner Verpackung weist darauf hin, dass das Produkt nicht über den normalen Hausmüll entsorgt werden darf. Benutzer sind verpflichtet, die Altgeräte an einer Rücknahmestelle für Elektro- und Elektronik-Altgeräte abzugeben. Die getrennte Sammlung und ordnungsgemäße Entsorgung Ihrer Altgeräte trägt zur Erhaltung der natürlichen Ressourcen bei und

garantiert eine Wiederverwertung, die die Gesundheit des Menschen und die Umwelt schützt. Informationen dazu, wo Sie Rücknahmestellen für Ihre Altgeräte finden, erhalten Sie bei Ihrer Stadtverwaltung, den örtlichen Müllentsorgungsbetrieben oder im Geschäft, in dem Sie das Gerät erworben haben.

Greek notice

Απόρριψη άχρηστου εξοπλισμού από χρήστες σε ιδιωτικά νοικοκυριά στην Ευρωπαϊκή Ένωση

Το σύμβολο αυτό στο προϊόν ή τη συσκευασία του υποδεικνύει ότι το συγκεκριμένο προϊόν δεν πρέπει να διατίθεται μαζί με τα άλλα οικιακά σας απορρίμματα. Αντίθετα, είναι δική σας ευθύνη να απορρίψετε τον άχρηστο εξοπλισμό σας παραδίδοντάς τον σε καθορισμένο σημείο συλλογής για την ανακύκλωση άχρηστου ηλεκτρικού και ηλεκτρονικού εξοπλισμού. Η ξεχωριστή συλλογή και ανακύκλωση του άχρηστου εξοπλισμού σας κατά την απόρριψη θα συμβάλει στη διατήρηση των φυσικών πόρων και θα διασφαλίσει ότι η ανακύκλωση γίνεται με τρόπο που προστατεύει την ανθρώπινη υγεία και το περιβάλλον. Για περισσότερες πληροφορίες σχετικά με το πού μπορείτε να παραδώσετε τον άχρηστο εξοπλισμό σας για ανακύκλωση, επικοινωνήστε με το αρμόδιο τοπικό γραφείο, την τοπική υπηρεσία διάθεσης οικιακών απορριμμάτων ή το κατάστημα όπου αγοράσατε το προϊόν.

Hungarian notice

Készülékek magánháztartásban történ selejtezése az Európai Unió területén

A készüléken, illetve a készülék csomagolásán látható azonos szimbólum annak jelzésére szolgál, hogy a készülék a selejtezés során az egyéb háztartási hulladéktól eltér módon kezelend . A vásárló a hulladékká vált készüléket köteles a kijelölt gy jt helyre szállítani az elektromos és elektronikai készülékek újrahasznosítása céljából. A hulladékká vált készülékek selejtezéskori begy jtése és újrahasznosítása hozzájárul a természeti er források meg rzéséhez, valamint biztosítja a selejtezett termékek környezetre és emberi egészségre nézve biztonságos feldolgozását. A begy jtés pontos helyér l b vebb tájékoztatást a lakhelye szerint illetékes önkormányzattól, az illetékes szemételtakarító vállalattól, illetve a terméket elárusító helyen kaphat.

Italian notice

Smaltimento delle apparecchiature da parte di privati nel territorio dell'Unione Europea

Questo simbolo presente sul prodotto o sulla sua confezione indica che il prodotto non può essere smaltito insieme ai rifiuti domestici. È responsabilità dell'utente smaltire le apparecchiature consegnandole presso un punto di raccolta designato al riciclo e allo smaltimento di apparecchiature elettriche ed elettroniche. La raccolta differenziata e il corretto riciclo delle apparecchiature da smaltire permette di proteggere la salute degli individui e l'ecosistema. Per ulteriori informazioni relative ai punti di raccolta delle apparecchiature, contattare l'ente locale per lo smaltimento dei rifiuti, oppure il negozio presso il quale è stato acquistato il prodotto.

Latvian notice

Nolietotu iek rtu izn cin šanas noteikumi lietot jiem Eiropas Savien bas priv taj s m jsaimniec b s

Š ds simbols uz izstr d juma vai uz t iesai ojuma nor da, ka šo izstr d jumu nedr kst izmest kop ar citiem sadz ves atkritumiem. J s atbildat par to, lai nolietot s iek rtas tiktu nodotas speci li iek rtotos punktos, kas paredz ti izmantoto elektrisko un elektronisko iek rtu sav kšanai otrreiz jai p rstr dei. Atseviš a nolietoto iek rtu sav kšana un otrreiz j p rstr de pal dz s saglab t dabas resursus un garant s, ka š s iek rtas tiks otrreiz ji p rstr d tas t d veid , lai pasarg tu vidi un cilv ku vesel bu. Lai uzzin tu, kur nolietot s iek rtas var izmest otrreiz jai p rstr dei, j v ršas savas dz ves vietas pašvald b , sadz ves atkritumu sav kšanas dienest vai veikal , kur izstr d jums tika nopirkts.

Lithuanian notice

Vartotoj iš priva i nam ki rangos atliek šalinimas Europos S jungoje

Šis simbolis ant gaminio arba jo pakuot s rodo, kad šio gaminio šalinti kartu su kitomis nam kio atliekomis negalima. Šalintinas rangos atliekas privalote pristatyti speciali surinkimo viet elektros ir elektronin s rangos atliekoms perdirbti. Atskirai surenkamos ir perdirbamos šalintinos rangos atliekos pad s saugoti gamtinius išteklius ir užtikrinti, kad jos bus perdirbtos tokiu b du, kuris nekenkia žmoni sveikatai ir aplinkai. Jeigu norite sužinoti daugiau apie tai, kur galima pristatyti perdirbtinas rangos atliekas, kreipkit s savo seni nij , nam kio atliek šalinimo tarnyb arba parduotuv , kurioje sigijote gamin .

Polish notice

Pozbywanie si zu ytego sprz tu przez u ytkowników w prywatnych gospodarstwach domowych w Unii Europejskiej

Ten symbol na produkcie lub jego opakowaniu oznacza, e produktu nie wolno wyrzuca do zwykłych pojemników na mieci. Obowi zkiem u ytkownika jest przekazanie zu ytego sprz tu do wyznaczonego punktu zbiórki w celu recyklingu odpadów powstałych ze sprz tu elektrycznego i elektronicznego. Osobna zbiórka oraz recykling zu ytego sprz tu pomog w ochronie zasobów naturalnych i zapewni ponowne wprowadzenie go do obiegu w sposób chroni cy zdrowie człowieka i rodowisko. Aby uzyska wi cej informacji o tym, gdzie mo na przekaza zu yty sprz t do recyklingu, nale y si skontaktowa z urz dem miasta, zakładem gospodarki odpadami lub sklepem, w którym zakupiono produkt.

Portuguese notice

Descarte de Lixo Elétrico na Comunidade Européia

Este símbolo encontrado no produto ou na embalagem indica que o produto não deve ser descartado no lixo doméstico comum. É responsabilidade do cliente descartar o material usado (lixo elétrico), encaminhando-o para um ponto de coleta para reciclagem. A coleta e a reciclagem seletivas desse tipo de lixo ajudarão a conservar as reservas naturais; sendo assim, a reciclagem será feita de uma forma segura, protegendo o ambiente e a saúde das pessoas. Para obter mais informações sobre locais que reciclam esse tipo de material, entre em contato com o escritório da HP em sua cidade, com o serviço de coleta de lixo ou com a loja em que o produto foi adquirido.

Slovakian notice

Likvidácia vyradených zariadení v domácnostiach v Európskej únii

Symbol na výrobku alebo jeho balení ozna uje, že daný výrobok sa nesmie likvidova s domovým odpadom. Povinnos ou spotrebite a je odovzda vyradené zariadenie v zbernom mieste, ktoré je ur ené na recykláciu vyradených elektrických a elektronických zariadení. Separovaný zber a recyklácia vyradených zariadení prispieva k ochrane prírodných zdrojov a zabezpe uje, že recyklácia sa vykonáva spôsobom chrániacim udské zdravie a životné prostredie. Informácie o zberných miestach na recykláciu vyradených zariadení vám poskytne miestne zastupite stvo, spolo nos zabezpe ujúca odvoz domového odpadu alebo obchod, v ktorom ste si výrobok zakúpili.

Slovenian notice

Odstranjevanje odslužene opreme uporabnikov v zasebnih gospodinjstvih v Evropski uniji

Ta znak na izdelku ali njegovi embalaži pomeni, da izdelka ne smete odvre i med gospodinjske odpadke. Nasprotno, odslužено opremo morate predati na zbirališ e, pooblaš eno za recikliranje odslužene elektri ne in elektronske opreme. Lo eno zbiranje in recikliranje odslužene opreme prispeva k ohranjanju naravnih virov in zagotavlja recikliranje te opreme na zdravju in okolju neškodljiv na in. Za podrobnejše informacije o tem, kam lahko odpeljete odslužено opremo na recikliranje, se obrnite na pristojni organ, komunalno službo ali trgovino, kjer ste izdelek kupili.

Spanish notice

Eliminación de residuos de equipos eléctricos y electrónicos por parte de usuarios particulares en la Unión Europea

Este símbolo en el producto o en su envase indica que no debe eliminarse junto con los desperdicios generales de la casa. Es responsabilidad del usuario eliminar los residuos de este tipo depositándolos en un "punto limpio" para el reciclado de residuos eléctricos y electrónicos. La recogida y el reciclado selectivos de los residuos de aparatos eléctricos en el momento de su eliminación contribuirá a conservar los recursos naturales y a garantizar el reciclado de estos residuos de forma que se proteja el medio ambiente y la salud. Para obtener más información sobre los puntos de recogida de residuos eléctricos y electrónicos para reciclado, póngase en contacto con su ayuntamiento, con el servicio de eliminación de residuos domésticos o con el establecimiento en el que adquirió el producto.

Swedish notice

Bortskaffande av avfallsprodukter från användare i privathushåll inom Europeiska Unionen

Om den här symbolen visas på produkten eller förpackningen betyder det att produkten inte får slängas på samma ställe som hushållssopor. I stället är det ditt ansvar att bortskaffa avfallet genom att överlämna det till ett uppsamlingsställe avsett för återvinning av avfall från elektriska och elektroniska produkter. Separat insamling och återvinning av avfallet hjälper till att spara på våra naturresurser

och gör att avfallet återvinns på ett sätt som skyddar människors hälsa och miljön. Kontakta ditt lokala kommunkontor, din närmsta återvinningsstation för hushållsavfall eller affären där du köpte produkten för att få mer information om var du kan lämna ditt avfall för återvinning.

Glossary

This section defines the terms used to describe the ASM user interface and program features.

Actions pane The right pane in the main window of the ASM user interface that provides a list of actions, based on your current selection in the Content pane. Along with other selectable items, the Actions pane provides access to storage-allocation wizards, which help you allocate and configure storage.

Advanced window A window accessed by clicking the Advanced button in any of the storage-allocation wizards or the Allocate Space Wizard. When accessed from any of the storage-allocation wizards, the Advanced window allows you to change the size of the allocated space and the default (recommended) advanced configuration settings. When accessed from the Allocate Space Wizard, the Advanced window allows you to change the size of the allocated space, percent full warning threshold, and enforced allocated limit (shared folders only).

allocated space Storage space that is being used by, or reserved for, application or shared folder storage.

application server A server computer in a computer network dedicated to running certain software applications whose job is to provide network access to software client/server applications and, sometimes, the data that belongs to applications as well.

array Also known as a JBOD (just a bunch of disks). A group of hard drives in an enclosure (chassis) that are controlled by an array controller.

array controller Controls reads and writes to the hard drives in an array.

backups A read-only copy of data copied to media, such as hard drives or magnetic tape, for data protection.
A full backup copies all the data selected to be backed up. An incremental backup copies only data selected to be backed up that has changed since the last full backup.
Backups provide data protection in the event of system or hard drive failure, because the data is stored on media separate from the system hard drives.

backup application An application used to create, manage, and monitor backups.

CIFS Common Internet file system. The protocol used in Windows environments for shared folders.

Content pane The center pane in the main window of the ASM user interface that displays storage utilization, and the storage status of application components and shared folders.

data migration The process of moving data from one storage device to another, such as moving application data from an application server to your HP All-in-One Storage System. ASM supports automatic data migration for Exchange and SQL Server data.

data protection Protects data from being corrupted or lost as a result of hard drive failure. Methods used to provide data protection include RAID and backups.

enforce allocated limit (quota) An enforced quota for the amount of storage available to a shared folder. An enforce allocated limit prevents data from being saved to a shared folder once all the storage space allocated to the shared folder is used.

Exchange storage group The fundamental unit of storage management in Microsoft Exchange. Storage groups consist of Mail stores, Public stores, and log files.

exclusive storage An Advanced window option that allows you to dedicate a hard drive(s) for storing data for a specific application component or shared folder.

file system A method for storing and organizing computer files and the data they contain to make it easy to find and access them.

hot spares An Advanced window option that allows you to reserve one or two hard drives as spares. A hot spare is a hard drive reserved as a spare for storage space configured as RAID 1, RAID 1+0(10), or 5. A hot spare automatically replaces a hard drive when it fails.

iSCSI Internet small computer system interface. Like an ordinary SCSI interface, iSCSI is standards-based and efficiently transmits block-level data between a host computer (such as a server that hosts Exchange or SQL Server) and a target device (such as an HP All-in-One Storage System). By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances.
ASM works with the Microsoft iSCSI Target, which builds the iSCSI infrastructure on application servers with data hosted on your HP All-in-One Storage System and on your HP All-in-One Storage System so that application data is stored on your HP All-in-One Storage System.

iSCSI LUN A type of LUN (logical disk) created on an application server by ASM when a storage-allocation wizard is ran to host application storage. When application storage is hosted using ASM, all storage communication passes through the iSCSI LUN on the application server to the LUN on your HP All-in-One Storage System. This allows data saved by the application to the iSCSI LUN on the application server to be transparently stored on your HP All-in-One Storage System instead.

log file The component of a Microsoft Exchange storage group or a Microsoft SQL Server database that contains log data.

logical disk Also known as a LUN. A logical disk contains one or more volumes and spans multiple hard drives in an array. RAID configuration of storage is performed at the logical disk level.

LUN Also known as a logical disk. ASM will grow a LUN (make it larger) when the LUN requires more of the storage space on an array.

Mail store The component of a Microsoft Exchange storage group that contains mailbox data.

Menu bar The horizontal menu located at the top of the ASM user interface. The menu bar is the Microsoft Management Console menu bar; ASM is a snap-in hosted by the Microsoft Management Console.

MMC snap-in Microsoft Management Console snap-in. An application added to the Microsoft Management Console. All-in-One Storage Manager is a MMC snap-in.

NAS Network-attached storage. This term is used to refer to a specialized type of file server. The HP All-in-One Storage System provides NAS storage as well as iSCSI storage.

Navigation pane The left pane in the main window of the ASM user interface that allows you to quickly navigate between HP All-in-One Storage System Management applications.

NFS Network file system. The protocol used in most Unix environments to share folders or mounts. The Create a Shared Folder Wizard does not create NFS shares, but NFS shares can be created using the Shared Folder MMC snap-in.

percent full warning threshold Percentage of capacity for a storage area (storage allocated to an application component or shared folder) at which an alert is generated. This alert is displayed in the Content pane and sent to the Windows Event Log. See Setting a percent full warning threshold on page 74 for more information.

Public store The component of a Microsoft Exchange storage group that contains public folder data.

RAID Redundant array of intelligent disks. Two or more hard drives configured to provide a storage with resilience to hard drive failure through the use of RAID striping and parity disks.

RAID level See Table 20 on page 73 for RAID level descriptions.

RAID striping Writing data to hard drives in an array by interleaving bytes or groups of bytes across the multiple hard drives. This allows more than one disk to be read from or written to simultaneously, which increases the performance.

RAID stripe size The number of bytes or kilobytes of data in a RAID stripe (block of data).

restore To recover lost data using a backup.

revert To return stored data to a previous state using a snapshot.

scaling Changes the display proportions of application component and shared folder storage in the Content pane. You can choose to scale by the size (capacity) of the application component and shared folder's storage space, or scale them all the same. To change the scale setting, select Tools > Options.

size The amount of storage that ASM allocates and configures for an application component or shared folder. To change the size of the allocated storage for an application component or shared folder, select the application component or shared folder in the Content pane and then select **Allocate Space** in the Actions pane.

snapshot A read-only copy of a volume at a specific point in time. Unlike a backup, data is not copied to any media during a snapshot. Instead, when a file is modified after a snapshot is created, the new updates are written to a new location. The file-system maintains records and pointers to keep track of the snapshot data and file changes. A snapshot takes less than a second to create.

Status bar The area located at the bottom of the ASM user interface that displays server information and system alerts.

tape library An enclosure filled with magnetic tape cartridges, tape drives, and a robot(s). The tapes are electronically labeled for identification and stored in library slots when not in use. When data needs to be written or read from a tape, the robot loads the tape cartridge into an available tape drive in the library.

Task Viewer A window that displays completed tasks, scheduled tasks, and errors. To open the Task Viewer, select Tools > Task Viewer.

toolbar The area below the menu bar that contains icons for commonly-used commands. The toolbar is the Microsoft Management Console toolbar; ASM is a snap-in hosted by the Microsoft Management Console.

top-level share Top-level shared folder in a directory hierarchy.

unallocated space Unused storage that is not allocated. Unallocated space includes raw (unconfigured) storage and unused configured storage (logical disks).

user-defined application Any remote application that runs under Windows Server 2003 and uses NTFS volumes for storage.

virtual array Hard drives in an array can be divided into groups to create two or more virtual arrays. ASM grows a virtual array (makes it bigger) when a hard drive(s) must be added to the virtual array to obtain the required storage space. A virtual array contains one or more LUNs.

virtual library Also known as a virtual tape library. A virtual library acts like a physical tape library except that hard drive arrays are used for storage instead of magnetic tapes.

volume Resides on a logical disk. Volumes are assigned a drive letter on the file system and contain file directories.

warning threshold See percent full warning threshold.

Index

A

accessing
  All-in-One Management Console, 23
accessing application and shared folder properties, 94
accessing application server properties, 108
accessing properties
  for SQL Server, 99
  for application server volumes, 108
  for Exchange, 94
  for HP All-in-One Storage System logical disks, 106
  for HP All-in-One Storage System volumes, 106
  for shared folders pools, 98
  for the user-defined application pool, 101
accessing storage area properties, 106
ACL, defining, 151
Active Directory Lookup, 161
ActiveX
  enabling, 24
All-in-One Management Console
  Remote Desktop method, 26
All-in-One Management Console
  iLO 2 method, 29
  direct attach method, 23
  remote browser method, 24
  remote server access, 23
Application Server View, 108
application server volumes
  operating status values, 109
  Storage properties, 109
Application Server View, 93
application server volumes
  accessing properties, 108
application servers
  managing storage, 53
application storage
  infrastructure, 54
Application Storage Manager
  alerts, 112
  Main window, 56
  user interface options, 58
Application View, 93, 93
Array Configuration Utility, 126
array controller, purpose, 47
arrays, defined, 47
audience, 15

B

backup, printer, 159
backup, with shadow copies, 143
basic disks, 49
basic disks, 49, 50
battery replacement notice, 187
boot sequence, 23

C

cables, 184
cache file, shadow copies, 134
CIFS, share support, 151
Class A equipment, 183
Class B equipment, 183
configuration
  Internet, 181
  network, 20
  server, 30
  worksheet, 32
conventions
  document, 15
  text symbols, 16
customer self repair, 17

D

data protection, 103
data blocks, 47
Data file properties, 101
data protection, 95
data striping, 47
default login, 24
Details properties
  Exchange storage groups, 95
DHCP, 30
Disk Management
  extending volumes, 130
document
  conventions, 15
  related documentation, 15

documentation
HP website, 15
providing feedback, 18
dynamic disks
clustering, 50
spanning multiple LUNs, 49

E

electrostatic discharge, 188
European Union notice, 185
expanding storage
Array Configuration Utility, 130
extending volumes
Disk Management, 130

F

factory image, 22
fault tolerance, 48
FCC notice, 183
File and Print Services for NetWare.
See FPNW
file level permissions, 144
file recovery, 141
file screening management, 152
File Server Resource Manager, 124, 152
file system elements, 50
file-sharing protocols, 50
files, ownership, 149
firmware updates, 118
folder management, 144
folder recovery, 141
folders
auditing access, 147
managing, 144
FPNW
accessing, 174
described, 173
installing, 173

G

grounding methods, 188
groups, adding to permissions list, 145

H

help
obtaining, 17
host configuration protocols, DHCP and non-DHCP, 30
HP
All-in-One Management Console, 124, 152, 163
Array Configuration Utility, 126
Storage Manager, 126
technical support, 17
Web Jetadmin, 156
HP All-in-One Storage System alerts
operating status values, 106
HP All-in-One Storage System logical disks
accessing properties, 106
Storage properties, 107
HP All-in-One Storage System volumes
accessing properties, 106
Storage properties, 108

I

iLO 2
See Integrated Lights-Out 2
iLO 2 method
connecting to network, 29
installation
planning, 19
server, 21
Integrated Lights-Out 2, described, 29
international notices and statements, 185
Internet
automatic configuration, 181
proxy server, 181
set up, 181

K

kernel-mode drivers
check for, 158
kernel-mode drivers
installation blocked, 158
kit contents, 21

L

laser compliance, 184
Lights-Out 100, described, 28
LO100
See Lights-Out 100
log file properties for database, 101
log properties for storage groups, 98
logical storage elements, 50
logical storage elements, 48
LUNs
described, 49

M

Mailstore database, 96

managing storage
for application servers, 53
for shared folders, 54
Microsoft Exchange Server
operating status values, 95
Microsoft Exchange storage group components
Storage properties, 96
Microsoft Exchange storage groups
Details properties, 95
Microsoft Exchange Server
accessing properties, 94
Microsoft Print Management Console, 156
Microsoft Printer Migrator, 159
monitoring storage, 93
mount points
not supported with NFS, 49
mount points
creating, 49
mounted drives and shadow copies, 134

N

NCP, creating new share, 178, 178
Nested Shares, 99
NetWare
adding local users, 176
enabling user accounts, 176
installing services for, 173
supervisor account, 177

O

operating status values
application server volumes, 109
Exchange, 95
HP All-in-One Storage System alerts, 106
shared folders, 98
user-defined applications, 102
operating system problems, 111

P

partitions
extended, 49
primary, 49
permissions
file level, 144
list
adding users and groups, 145
removing users and groups, 145
modifying, 146
resetting, 146
physical configuration, 22
physical storage elements, 46
planning
configuration checklist, 20
installation, 19
network access method, 19
network configuration, 20
power cords, 187
power on
server, 22
print services for UNIX, 170
printer backup, 159
PublicStore database, 97

Q

quota management, 152

R

rack stability
warning, 16
RAID
data striping, 47
LUNs in volumes, 49
summary of methods, 48
Rapid Setup Wizard, 32
recovering from logical disk failure, 117
regulatory compliance, 183
related documentation, 15
remote access
Telnet Server, 27
remote browser method
connecting to network, 25
Remote Desktop method
connecting to network, 26
Remote management, 28

S

safety, 187
SAS/SATA hard drives
LEDs, 43
Search enhancements, 124
security
auditing, 147
file level permissions, 144
ownership of files, 149
serial number, 21
server
AiO400t hardware components, 37
doocumentation, 118
installation, 21
power on, 22
Server for NFS
described, 163

Server for NFS
Authentication DLL, 163
Service for User
for Active Domain controllers, 163
services for AppleTalk, installing, 179
Services for UNIX, 49, 51
set up
Internet, 181
setting up
overview, 19
setup completion, 32
shadow copies
mounted drives, 134
shadow copies, 50
backups, 143
cache file, 134
defragmentation, 133
described, 131
disabling, 138
file or folder recovery, 141
managing, 134
on NFS shares, 141
on SMB shares, 140
planning, 131
redirecting, 137
scheduling, 136
uses, 131
viewing list, 136
Shadow Copies for Shared Folders, 139
share management, 150
shared folder storage infrastructure, 55
shared folders
operating status values, 98
Storage properties, 105, 105
shared folders pool
accessing properties, 98
shares
administrative, 151
creating new NCP, 178, 178
managing, 150
NCP, 177
standard, 151
Single Instance Storage, 123
SQL Server
accessing properties, 99
SQL Server database components
Storage properties, 101
SQL server errors, 112
SQL Server properties
operating status values, 100
startup
collecting information, 30
status icons, 93
storage configurations, 22
Storage properties
Exchange storage group components, 96
storage management
elements, 45
overview, 45
process, 46
storage management infrastructure, 53
Storage Manager for SANs, 123
Storage properties
shared folders, 105, 105
SQL Server database components, 101
storage reports, 153
Storage View, 93, 105
Subscriber's Choice, HP, 17
Subscriber's Choice, 118
symbols in text, 16
system updates, 117

T

technical support
web site, 118
technical support
HP, 17
service locator website, 18
Telnet Server
enabling, 27
sessions information, 27
Telnet Server, 27
text symbols, 16
troubleshooting, 111

U

UNIX, print services, 170
user-defined application pool
accessing properties, 101
user-defined applications
operating status values, 102
storage properties, 103
user-mode drivers, 158
users
adding to permission list, 145
NetWare
adding, 176
enabling, 176

V

Volume Shadow Copy Service, 131
volumes
creating Novell, 173
NCP, 177
planning, 49
vssadmin tool, 134

W

warning
  rack stability, 16
Warning Threshold, 96
WEBES (Web Based Enterprise Services, 118
websites
  customer self repair, 17
  HP , 18
  HP Subscriber's Choice for Business, 17
  product manuals, 15
WEEE directive, 188